Xavier Raufer

# Cyber-criminologie

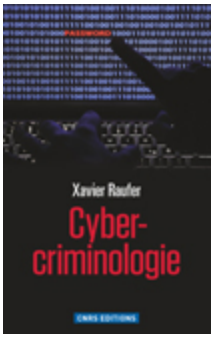
CNRS EDITIONS

Xavier Raufer

# Cyber-criminologie

CNRS EDITIONS

**L'ampleur enfin révélée de la criminalité organisée dans le cyber-monde**




« L'univers cybernétique est désormais l'un des principaux domaines de la fraude et du crime », a déclaré un expert anglais à la suite du piratage de 233 millions de fiches clients d'un géant du e-commerce. Aujourd'hui, les victimes de la cyber-criminalité se comptent par dizaines de millions, des stars d'Hollywood aux habitués des réseaux sociaux ou du commerce en ligne. Comment, à partir de quels ordinateurs et de quelles techniques les nouveaux gangs du net opèrent-ils ? C'est ce que révèle le nouveau livre de Xavier Raufer. Fondé sur des informations seulement connues des spécialistes, *Cyber-criminologie* dévoile la gravité d'un phénomène qui menace le citoyen ordinaire, les grandes entreprises, les États, les banques, etc. Piratage et vente clandestine de données personnelles, maliciels pénétrant les ordinateurs publics et privés, fraudes identitaires ou à la carte bancaire, sites marchands illicites cachés dans le *dark web* : le monde du cyber-crime est aussi florissant qu'insaisissable.

Xavier Raufer explique ici comment notre société hyper-connectée a donné naissance à un cyber monde où prolifèrent hackers, mafias du net russes, chinoises ou iraniennes, *hacktivists* libertaires exploitant les failles de nos systèmes informatiques. Sans parler de la surveillance omniprésente des États comme l'affaire Prism l'a révélé. Des dangers qui vont de pair avec la croissance exponentielle du Net…

*Xavier Raufer, criminologue et enseignant à l'université Panthéon-Assas, est l'auteur de nombreux ouvrages dont* Les nouveaux dangers planétaires *(Biblis)*.

Xavier Raufer

# Cyber-criminologie

CNRS ÉDITIONS
15, rue Malebranche – 75005 Paris

## Du même auteur (depuis 2010)

(Ouvrages de l'auteur jusqu'à 2010 : voir le site www.xavier-raufer.com)

*Criminologie – la dimension stratégique et géopolitique*, Collection Sécurité Globale, Eska, 2014

*Géopolitique de la mondialisation criminelle*, *la face obscure de la mondialisation*, Presses Universitaires de France – 2013

*Les nouveaux dangers planétaires*, chaos mondial, décèlement précoce, CNRS Éditions, 2009 et Biblis, édition de poche, février 2011 – Ouvrage couronné par l'Académie française

*Quelles guerres après Oussama ben Laden ?* Plon, 2011

© CNRS Éditions, 2015

ISBN : 978-2-271-08560-3

*Ce document numérique a été réalisé par Nord Compo.*

*À la mémoire de Laurence I.*
*qui, la première, m'entraîna dans ce monde inouï.*

# Sommaire


Couverture

Titre

Du même auteur (depuis 2010)

Copyright

Dédicace

Quatre thèses fondatrices de la cyber-criminologie

Glossaire

Préambule

- Première partie - Champ de bataille et cadre large
- Deuxième partie - Les champs du cybercriminogène
- Troisième partie - Méandres et percées du cybercrime
- Quatrième partie - La cybercriminalité en action
- Cinquième partie - À l'horizon 2020, trois questions majeures
- Sixième partie - Prescrire

Conclusion

Annexes

Annexe I. Le Champ préalable d’inspection

Annexe II. Singularity (singularité technologique)

Annexe III. L’appareil de cyber-sécurité des États-Unis

Annexe IV. Les Européens et la cyber-sécurité

Annexe V. Les crypto-monnaies (CM) alternatives au bitcoin

Références, sources & citations

Achevé

# Quatre thèses fondatrices de la cyber-criminologie

• *Diagnostic 1* – Dans l'ensemble « cybercrime », crime domine. Scruter le monde cybercriminel révèle que celui-ci n'a rien inventé d'original. Dans leur propre milieu et jusqu'à présent, les cybercriminels se bornent à reproduire les variantes de la criminalité physique.

• *Diagnostic 2* – La cybercriminalité ne régressera pas grâce à plus encore de haute technologie, mais par volonté politique. Une simple fuite en avant de type blindage-et-canon provoquerait, dans ce domaine, un désastre analogue à celui de l'inepte guerre *high-tech* d'Irak.

• *Traitement 1* – Il faut au cybermonde un code de la route comme, en son temps, la société de l'automobile suscita le sien. Ce code devra être conçu et imposé par une coalition de nations puissantes, dans l'espoir raisonnable qu'il s'imposera mondialement. Autre image possible pour l'indispensable superstructure normative : celle de la tour de contrôle.

• *Traitement 2* – Le code de la route vaut pour tout véhicule, luxueux ou modeste : de même, seul un code du cybermonde sanctionnera-t-il efficacement les prédateurs, financiers maraudeurs, géants du net, etc. qui, aujourd'hui, le pillent impunément ou exploitent ses usagers.

# Glossaire

*Ce glossaire n'a nulle prétention encyclopédique. Il vise simplement à faciliter l'accès au texte en traduisant et/ou définissant des mots, concepts & acronymes peu familiers aux non-spécialistes.*

*Les définitions et expressions originales en langue anglaise (émanant de sources officielles anglo-saxonnes) ont été traduites par l'auteur.*

**Anonymous** : Groupe hacktiviste (voir ce terme, plus bas) déstructuré et protoplasmique, sans hiérarchie ni autorité centrale. Son slogan est : « Nous sommes légion. Nous ne pardonnons pas. Nous n'oublions pas. Craignez-nous », et son icône, le masque de Guy Fawkes, est désormais bien connu. Fondé en 2003 dans un esprit libertaire de type Robin des Bois, Anonymous multiplie depuis les cyberattaques sur des cibles estimées malfaisantes ou dictatoriales : l'Église de Scientologie, informatiquement harcelée par de mauvaises blagues ; attaques DDoS (voir ce terme, plus bas) contre les systèmes de paiement en ligne, Paypal, etc. qui bloquent des contributions financières à Wikileaks et aux grands « lanceurs d'alerte » comme J. Assange, E. Snowden, etc. ; attaques des sites du gouvernement tunisien lors du « printemps arabe ». Pendant le conflit dans la Bande de Gaza en juillet-août 2014, Anonymous, indigné par les massacres de civils, attaque divers sites officiels israéliens, dont celui du Mossad, de l'armée, du Premier ministre, du Conseil national de sécurité et du ministère de la Justice.

**AET (Advanced Evasion Techniques**, techniques de contournement avancées) : « déguisement » pour pénétrer les cibles (sites, réseaux, systèmes) et y actionner ensuite des logiciels pirates. Logiciel malveillant (*malware*) polymorphe, aux multiples potentialités dangereuses, l'AET

pénètre en douceur sa cible en plusieurs points ou plusieurs fois. Ces éléments sont d'apparence innocente et ne sont pas reconnus comme dangereux par les systèmes de protection (coupe-feu) de l'ordinateur (IDS, Intrusion Detection Systems, voir ce terme). Une fois « dans la place » et selon de multiples agencements, l'AET recompose ses divers éléments, pour ensuite saboter, piller, etc. Les premiers AET ont été signalés en 2010.

**APT (Advanced Persistent Threat)** : attaque informatique ciblée et sophistiquée dont les auteurs ont les moyens et le temps d'arriver à leurs fins. Complexe et menée par des pirates experts, l'APT cherche en général à siphonner des bases de données.

**Backoff** : redoutable maliciel (ou *malware*, voir plus bas ce terme) repéré pour la première fois en octobre 2013. Dans la mémoire d'un ordinateur cible, Backoff siphonne toutes les données concernant les cartes de paiement (qu'ensuite, le pirate n'a plus qu'à vendre), lit les frappes du clavier pour y copier les mots de passe et, surtout, installe au cœur du système une trappe pour conserver l'accès à l'ordinateur cible, s'il « crashe » ou est réinitialisé. Cette trappe rend sans cesse Backoff améliorable et modifiable.

**Big Data** : océan toujours plus illimité de données rassemblées dans le Cloud (voir ce terme plus bas). Milliards et milliards de traces numériques (chiffres, textes, images, photos, etc.) laissées par qui use d'une carte de paiement, d'un smartphone, consulte Internet, achète en ligne, etc. Big Data permet l'analyse de données par masses énormes et à très grande échelle, en théorie pour améliorer le suivi des clients, anticiper les besoins du marché ou favoriser les échanges entre objets connectés. Mais derrière les chiffres et propos extatiques, Big Data constitue sans doute le plus grand système de surveillance jamais imaginé, au service de certains gouvernements et des géants du net. Notons que depuis août 2014, la Commission générale de terminologie et de néologie, chargée de favoriser l'enrichissement de la langue française, demande de dire « mégadonnées » et non plus big data.

**Bitcoin** : cybermonnaie, ou devise numérique, lancée en 2009. Dès son origine, elle séduit à la fois les internautes d'orientation libertaire et les *fans* de high-tech. Pour ses promoteurs, bitcoin est destiné à devenir un système

alternatif de paiement – peut être la vraie monnaie mondialisée qu'attendrait, selon eux, le XXI$^{e}$ siècle. Mais en fait, bitcoin a d'abord intéressé les criminels. Fondée sur un système de pénurie organisée, intraçable et gérée par un vaste réseau centralisé, bitcoin ne dépassera jamais les 21 millions d'unités – d'où, sa forte volatilité. En juin 2014, on en comptait quelque 13 millions en circulation et un bitcoin valait environ 600 dollars.

**Black Hat** : dans le registre gentils/méchants, Silicon Valley reconnaît deux sortes de hackers, ou pirates, les *white hat*, n'ayant pas d'objectifs illicites mais au contraire l'intention positive d'améliorer le cybermonde ; et les *black hat*, qui eux, piratent pour voler, saboter, etc. Depuis 1997, se tient chaque année à Las Vegas une Black Hat convention – qui devrait plutôt se nommer « White Hat Convention » mais les pirates attirent les foules – où convergent des milliers d'informaticiens et d'experts en sécurité, pour présenter et vanter leurs intrusions les plus spectaculaires, étudier les cyber-risques émergents et tenter d'améliorer la sûreté des systèmes et réseaux.

**Botnet** : réunit les deux mots anglais roBOT et NETwork (robot et réseau). Ce dispositif informatique assemble en un réseau des ordinateurs « kidnappés » à distance, à partir desquels les pirates accomplissent ensuite des actes malveillants, comme des envois de Spam ou des attaques type DDoS (voir plus bas ces deux termes).

**Chiffrage/cryptage** : le plus souvent, il consiste à transformer un texte clair en une suite de signes apparemment privée de tout sens. Conduite à l'aide d'une clé secrète, cette opération mathématique vise à produire un document final chiffré, incompréhensible à tout autre que son destinataire. Au total, le chiffrage répond à trois besoins : authentification (l'auteur est le vrai) ; intégrité (le texte n'a pas été altéré) ; confidentialité (le tiers indésirable n'y a pas accès).

**Chief Information Security Officer (CISO)** : Aux États-Unis, c'est le responsable de la sécurité informatique d'une entreprise, d'une administration, etc. Une petite majorité des entreprises américaines de 1 000 employés et plus possède un CISO à temps plein ou partiel. On verra

plus bas que l'entreprise de grande distribution Target (la 3e des États-Unis), qui fut victime en 2013 d'un immense siphonnage ayant pu affecter jusqu'à un tiers des cartes de paiement du pays, n'a embauché un CISO qu'après la catastrophe. Attitude jusqu'ici fréquente pour des entreprises, même importantes. Voir aussi plus bas l'équivalent français RSSI : Responsable de la Sécurité des Systèmes d'Information.

**Cloud** : Dispositif d'informatique dématérialisé, au sein duquel les données et informations sont stockées dans des ensembles de serveurs connectés.

**CloudBot** : Des hébergeurs en ligne proposent souvent (à leurs débuts) des comptes gratuits sur le cloud pour séduire de nouveaux clients ; dans ces *data centers*, des développeurs peuvent stocker leurs travaux sans encombrer leurs propres serveurs. Or nombre de ces startups « Data Centers » ne demandent qu'une adresse courriel aux clients ainsi hébergés. Il suffit donc d'ouvrir une quinzaine de ces comptes puis d'assembler en un CloudBot l'espace de stockage ainsi acquis, (comme on le ferait dans le monde physique pour les wagons d'un train, derrière une locomotive), pour disposer gratuitement d'un superordinateur qui peut ensuite servir à lancer des attaques DDoS, « casser » des mots de passe, spéculer sur des monnaies numériques, etc.

**Computer Network Exploitation** : dans le langage de la NSA (voir la cinquième partie du livre) et du Cyber Command US, ce terme désigne toutes les cyberattaques et opérations visant à infiltrer des logiciels de contrôle dans des réseaux informatisés étrangers ; à s'y ménager des accès clandestins, pour y susciter et maintenir une présence. Objectif : en usant d'un cyber-arsenal secret, se livrer à des manipulations, sabotages, prises de contrôle, destructions, récupérations de données. Plus largement : obtenir des secrets militaires, du renseignement et intercepter des communications.

**CSIRT (Computer Security Incident Response Team), ou CERT (Computer Emergency Response Team)** : au niveau national ou régional, cellule/équipe d'alerte et de réaction aux attaques, piratages, etc.

**Cyberattaques** – définition du National Research Council, Washington, 2009 : « Opérations délibérées visant à altérer, perturber, tromper, dégrader ou détruire les dispositifs ou réseaux d'un système d'information et/ou les programmes résidant ou transitant par ces mêmes dispositifs ou réseaux ». Autre définition (*Yale Journal of International Affairs*, *cf*. références) : « Une cyberattaque vise à invalider les systèmes digitaux critiques des institutions centrales d'un État-nation : militaires, politiques, sociaux ou économiques ; ou encore utilise le cyberespace pour attaquer les infrastructures d'une société développée comme ses réseaux de transport d'énergie, ses systèmes financiers ou ses services d'urgence ». Une cyberattaque a de nombreux avantages : coût modeste, anonymat, large choix de cibles, frappes possibles de l'autre bout du monde, difficulté à identifier l'attaquant et à localiser l'origine réelle de l'attaque. À l'inverse de ces opportunités, la crainte majeure de tous les états-majors, cyber ou non, est le « Pearl Harbour électronique ».

Autre définition de la cyberattaque, en français : « agression illégale visant des ordinateurs ou des réseaux, ainsi que les informations et données qui y sont contenues, dans l'idée d'intimider ou de contraindre un gouvernement ou une population, pour un motif politique ou social. Cette attaque implique toute forme de violence contre des personnes ou des biens ; ou, au minimum, provoque assez de dégâts pour inspirer la crainte. Exemple : attaques entraînant la mort ou des blessures ; provoquant des accidents aériens, la contamination d'eau potable, des pertes économiques ou financières lourdes. Au-delà, toute attaque grave visant des infrastructures critiques ».

**Cyber-baronnies** (*robber barons*) : empires numériques comme Amazon, Facebook, Google, etc.

**Cybercrime** : Lors de sa Convention de Budapest, le Conseil de l'Europe a produit en 2001 (entrée en vigueur, 2004) le premier instrument juridique international opérationnel sur la cybercriminalité. En 2004, l'Organisation des États américains a produit une *Comprehensive inter-American strategy to combat threats to cyber-security*. Selon l'ONU Drogue & Crime (ONUDC), le « chiffre d'affaires » du cybercrime

représenterait 0,8 % du Produit Brut Mondial (PBM) ; le crime organisé hors cybercrime, 1,2 % du PBM et la piraterie maritime 0,2 % du PBM.

**Cyberespace** : L'ultime territoire hors contrôle – mais aussi 5e domaine des opérations militaires (terre, mer, air, espace, cyberespace) et lieu d'une possible « course au cyber-armements ». Voici la définition du ministère américain de la Défense en 2008 : « Domaine global de l'environnement informatif humain, formé de réseaux interdépendants au sein des infrastructures des technologies de l'information, incluant l'Internet, les réseaux de télécommunications, les dispositifs informatiques et leurs propres systèmes de traitement et de contrôle… Le royaume des réseaux informatisés, dans lesquels l'information est rangée, partagée et diffusée en ligne ».

**Cyber-espionnage** – définition du FBI : « Usage ciblé des ordinateurs visant à obtenir un quelconque secret ».

**Cyberguerre** – définition de l'US Air Force : « Capacité à détruire, interdire, dégrader, perturber ou tromper… Tout en se protégeant de pratiques hostiles au sein du cyberespace visant à un identique objectif ».

**Cybernétique** : science dont procèdent l'informatique et Internet. En grec ancien, *kubernesis* est l'art de tenir un gouvernail, plus largement de piloter les navires. Aujourd'hui, c'est la science des systèmes autorégulés et des interactions entre systèmes gouvernants (contrôle) et gouvernés (opérations).

**Cyberterrorisme** – définition du FBI : « Attaque préméditée et politiquement motivée visant des systèmes informatiques ou des dispositifs informationnels, des logiciels et des données, le tout résultant en des violences subies par des cibles civiles ; ces attaques étant commises par des entités humaines ou par des opérateurs clandestins ».

**Dark wallet** : service, logiciel, etc. illicitement conçu pour rendre et maintenir invisible toute transaction digitale (financière, d'abord).

**Dark web ou web profond** : apprentis sorciers voulant « chevaucher le tigre » ? Cyniques ? Comme on le verra tout au long des parties IV et V de cet ouvrage, le « web profond » fut créé par l'Amérique officielle, comme réseau entièrement privé et anonyme. Dix ans plus tard, ce paradis électronique du cybermonde – équivalent contemporain de la « cour des miracles » du Moyen Âge – regroupe une infinité de bases de données, forums et sites illicites, inaccessibles depuis les usuels moteurs de recherches. Sans doute trois fois plus vaste en volume que le web de surface, le *Dark web* est un cauchemar pour les États car, dans un anonymat quasi-parfait, il permet toutes les transactions criminelles sur les stupéfiants, les armes, la pédophilie, etc.

**Data broker** (fournisseur de données informatiques) : opaque et intrusive « industrie » de vente des données personnelles de citoyens ou consommateurs en vue d'actions de marketing.

**DDoS (Distributed Denial of Service)** : désormais classique, cette attaque informatique consiste à bombarder de messages non désirés, jusqu'à le submerger, un système cible, ses fonctions et connexions à Internet ; ce, grâce à des « cyber-meutes » (*Botnets*) rassemblant jusqu'à des milliers d'ordinateurs « capturés » et mis en ordre de bataille par des pirates. L'attaque DDoS peut aussi servir de cheval de Troie à des intrusions plus subtiles ; ou permet de les masquer. Produit par la société de sécurité informatique NSFocus, le rapport *DDoS threat focus*, annonce avoir mondialement recensé en 2013, 245 000 attaques DDoS, soit un peu plus de 670 par jour, ou 28 par heure.

« **Fullz** » (« complets » en argot anglais des hackers, sans doute par analogie avec « full » ou « full house » au poker, soit un brelan et une paire). Il s'agit de reconstituer toutes les données possibles (obtenues par piratage) sur un individu, soit nom, prénom, numéro de sécurité sociale, nom de jeune fille de la mère, etc. Tout ce qui permet de créer frauduleusement des dossiers d'obtention de cartes de paiement et de prêts personnels en vue de diverses fraudes ou escroqueries.

**GameoverZeuS** (ou GOZeuS, P2PZeuS) : célèbre « maliciel », présenté ici pour démontrer l'expertise des pirates informatiques. Lancé en

octobre 2011, le cheval de Troie GOZeuS a siphonné en deux ans une centaine de millions de dollars, notamment à de grandes banques. Démantelé en juin 2014 (lors de l'« Opération Tovar ») GOZeuS est en pleine « résurrection » depuis août 2014 et tente à nouveau de s'infiltrer dans réseaux, ordinateurs et serveurs des entreprises.

**Geek** : l'infanterie de Silicon Valley. Dans l'argot du milieu high-tech américain, le geek est un *digital native*, jeune adulte ou adolescent natif du cybermonde. Passionné d'électronique et d'informatique, le geek passe son temps dans l'univers numérique et devant des écrans. Chez les geeks, la croyance basique est que, dans la plupart des domaines, les cyber-machines peuvent faire mieux que l'être humain. Dans une rhétorique moins baba cool, le geek plus offensif mute parfois en *code warrior* (guerrier ou combattant du code).

**Giga serveur** : net-entreprise géante (Google, etc.), dans les domaines du commerce, de la finance, etc.

**Hacktiviste** : pirate motivé par l'idéologie ou le fanatisme, ciblant les sites qu'il considère comme « ennemis », pour les saboter ou les inonder de propagande hostile. Les hacktivistes peuvent aussi infecter leurs cibles par des virus malveillants, leur piller des données, des mots de passe, les bombarder de Spam, etc. Ni plus ni moins que le pirate-prédateur, la « boîte à outils » du hacktiviste se compose d'un ensemble de services et d'outils illicites (forums, etc.) ; d'un système de paiement anonyme type bitcoin ; enfin, d'un « refuge » sur le dark web où des hébergeurs tout aussi criminalisés lui fournissent des sites « blindés », le plus souvent hors d'atteinte des polices, justices, etc.

**HFT : High Frequency Trading** (transactions boursières à haute fréquence) : l'art d'user d'ordinateurs super-puissants et d'algorithmes sophistiqués pour conduire, en une fraction de seconde, des opérations de bourse (achat, vente…), au plus près possible de la vitesse de la lumière. Voir aussi plus bas « Transactions à haute fréquence – les risques ».

**HTTPS : HyperText Transfer Protocol Secure**, protocole de gestion des transactions sécurisées sur Internet.

**ICANN : Internet Corporation for Assigned names and Numbers**, organisme de régulation de l'Internet, fondé en 1998 aux États-Unis.

**IDS – Intrusion Detection Systems**, systèmes de détection des intrusions : s'agissant des « solutions » vendues dans le commerce, ces IDS ne sont le plus souvent qu'une fragile rangée de barbelés numériques, ou une nouvelle ligne Maginot. Selon le *Verizon Risk Report* de 2013, 62 % des pénétrations dans un réseau informatique restent indétectées pendant des mois, voire des années. Par exemple, pour le maliciel Backoff, même les antivirus parfaitement mis à jour, opérant sur des ordinateurs des plus « étanches » (*fully patched*), n'ont pu repérer ce maliciel ni alerter sur sa grande toxicité. Membre fondateur de la SSL Foundation, l'ingénieur et cryptographe Ben Laurie avertit sans cesse que les principaux logiciels de protection fonctionnent mal et produisent bien trop de fausses alertes (www.apache-ssl.org). De ce fait et aujourd'hui encore, la sécurité cybernétique d'une entreprise relève plutôt du travail à l'aveuglette : « Il n'y a pas de baguette magique en matière de lutte contre les intrusions. Il faut superposer par couches successives les technologies les plus efficaces, embaucher les meilleurs spécialistes puis compter sur la chance ». (« *The job that asks: can you hack it?* », *cf.* Références)

**Internet** : la scène mondiale du théâtre numérique. Inventée en 1973 à Palo Alto (Californie), grâce aux crédits d'une agence scientifique du Pentagone, la DARPA (Defense Advanced Research Projects Agency). Dispositif informatique simple et universel permettant d'échanger des informations digitales. Son principe de base : la connectivité entre tous.

**ITU – International Telecommunication Union** : organisation internationale de régulation des télécoms, fondée en 1865 comme International Telegraph Convention.

**Keylogger** (par exemple, dispositif KVM, ou Keyboard Video Mouse) : aisément achetables sur le dark web, ces maliciels espionnent et enregistrent les frappes sur les touches du clavier d'un ordinateur, ce qui permet par exemple d'y récupérer des mots de passe.

**Malware** – « maliciel » : logiciel toxique délibérément introduit dans un ordinateur, pour y voler des données confidentielles, ou s'y livrer à des opérations indésirables.

**Métadonnées** : pour un appel téléphonique, l'ensemble des métadonnées consiste en : numéro appelé, date, durée de l'appel et fréquence des appels analogues. Les métadonnées d'une photo numérique comprennent : l'auteur, la date de prise de vue, un titre, un ou des mot(s)-clé(s), le type d'appareil utilisé, etc. Plus largement, il s'agit d'un étiquetage des ressources numériques (textes, images…) en vue de classements et recherches ultérieurs. Pour Stewart Baker, directeur juridique de la NSA : « Les métadonnées vous disent absolument tout de la vie d'un individu. Si vous disposez d'assez de métadonnées, vous pouvez vous passer de contenu ». Commentaire du général Michael Hayden (ex-directeur de la CIA et de la NSA) : « C'est tout à fait correct ». Un professeur d'informatique de l'université de Princeton ajoute : « Naguère incapables d'exposer des informations privées, des données parcellaires désormais agrégées révèlent des faits sensibles sur nos vies quotidiennes ; faits que nous n'entendions ni ne souhaitions partager » (*New York Review Of Books, « Partial disclosure »*, *cf.* Références).

**NSA, National Security Agency** : agence américaine fédérale en charge de l'espionnage électronique. Créée en 1952 dans un tel secret que son ironique sobriquet est « No Such Agency ». Elle compterait aujourd'hui 30 000 fonctionnaires et 60 000 contractuels. Quand on l'interroge sur ses activités, la NSA se borne à répéter qu'elle « collecte ce que la loi l'autorise à collecter sur des cibles intéressantes, quel que soit le moyen technique employé par ces cibles ». Actuellement, la cour américaine secrète « Foreign Intelligence Surveillance Court » donne (à chaque fois, pour un an) la capacité à la NSA de cibler 193 pays (hors du groupe anglo-saxon dit des « Five Eyes » : Grande-Bretagne, Canada, Australie et Nouvelle-Zélande, hors des États-Unis) ; la NSA cible aussi le Fonds monétaire international, la Banque mondiale, l'Agence internationale pour l'énergie atomique et l'Union européenne. Comme objectifs précis, la NSA a surveillé en 2013, 90 000 entités ou individus.

**Open SSL** : fondé sur les protocoles TLS/SSL (voir plus bas), ce projet Open Source est conçu dans la décennie 1990. Ce sera un logiciel d'accès libre, non lucratif et participatif, visant à protéger les données sur Internet et plus largement, à y empêcher le piratage et l'espionnage. Chargée d'entretenir et d'améliorer ce projet, la OpenSSL Foundation vit de ses contributeurs volontaires, dans un esprit d'autorégulation.

**Phishing** (hameçonnage) : se faisant passer pour un conseiller de leur banque, un opérateur télécom, un technicien quelconque… voire pour le fisc, le pirate envoie à ses cibles des messages personnalisés destinés à les inquiéter, à les pousser à réagir – donc à lui répondre. Ayant ainsi soutiré des données confidentielles à assez de naïfs, et les plus complètes possibles (mots de passe, numéros de compte bancaire, etc.), le pirate les assemble en un « pack » de « Fullz », qu'il vend à d'autres malfaiteurs à des fins de fraude, d'escroquerie, etc.

**PIN (Personal Identification Number)** : code confidentiel protégeant l'accès à un site, à une carte de crédit, etc. Le vol d'un PIN permet en outre aux escrocs d'accéder à une foule d'informations personnelles – historiques d'achats, discussions sur des forums, adresses, photos – ce qui leur permet d'affiner leurs approches pour mieux tromper leurs victimes.

**RAT** (Remote Administration Tool, ou Trojan) : outil (ou cheval de Troie) de contrôle à distance. Le RAT (Blackshades par exemple, voir plus loin dans le texte) permet de prendre le contrôle d'un ordinateur, puis d'y faire ce qu'on veut : activer le micro ou la caméra, récupérer le contenu d'un disque dur, le coder (donc, le kidnapper) pour le restituer ensuite contre rançon ; capter les frappes du clavier (pour pirater les mots de passe), etc.

**Rétroingénierie** (*reverse engineering*) : la méthode de base employée par les pirates informatiques. La pratique de cette ingénierie inversée permet au pirate, qui n'a évidemment pas accès aux spécifications d'origine, d'étudier un système (logiciel, réseau…), pour en déterminer le mode de conception et ensuite s'y infiltrer, voire en prendre le contrôle.

**RSSI** : responsable de la Sécurité des Systèmes d'Information ; identique à CISO.

**SEPA** – Single Euro Payments Area : normes informatisées de paiement à l'intérieur de l'Union européenne (UE), usant des numéros de compte bancaires unifiés (BIC et IBAN) pour les virements et prélèvements. La Zone SEPA rassemble les 28 pays de l'UE, plus l'Islande, la Norvège, la Suisse, le Liechtenstein et Monaco.

**Serveur** : groupe plus ou moins important d'ordinateurs agencés en réseaux et interagissant entre eux.

**Singularity** (singularité) : important corpus idéologique de Silicon Valley, voir annexe II.

**SPAM** : messages électroniques non désirés par le récipiendaire, que des pirates adressent par millions à des adresses courriels volées, à des fins de publicité ou de propagande.

**TAILS** – The Amnesic Incognito Live System : outil d'anonymisation et de protection de la vie privée, dont l'usage efface toute trace de passage d'un internaute dans les ordinateurs hôtes (voir TOR, plus bas).

**TLS/SSL – Transport Layer Security/Secure Sockets Layer** : protocoles de codage des échanges sur Internet notamment utilisé par OpenSSL.

**TOR** – The Onion Router, routage en oignon : l'image des pelures superposées de l'oignon vient de ce que, sur le réseau TOR, les données cheminent en recevant à chaque étape une nouvelle couche de chiffrement, ce qui les rend non identifiables et non localisables. TOR abrite ainsi ses usagers de toute surveillance et analyse du trafic et anonymise totalement les échanges. Son utilisateur peut donc visiter le web incognito, mais aussi créer, sur le dark web, un site invisible aux engins de recherche ordinaires. Diffusé gratuitement, ce logiciel est entretenu par les volontaires internationaux de la fondation « TOR project ». En 2011 encore, 60 % du budget de TOR provenait malgré tout de deux ministères américains : les

Affaires étrangères (State Department) et la Défense (Pentagone). Au total, ce dispositif est si sophistiqué que même ses concepteurs prétendent ignorer comment le « craquer ». Pour comprendre comment fonctionne TOR, ou y accéder, voir <https://www.torproject.org> et <Tor2web.org>.

**Transactions à haute fréquence – les risques** (HFT, pour High Frequency Trading) : système automatisé ultrarapide de transactions en Bourse (dixièmes, voire centièmes de seconde) ; de ce fait le HFT, qualifié de « banditisme légal » par ses critiques, est quasi incontrôlable par l'homme. En 2014, le HFT concerne environ 50 % des achats et ventes d'actions américaines (70 % de ces transactions en 2009). Rappelons qu'il y a de multiples bourses aux États-Unis, dont 13 publiques (comme le New York Stock Exchange, NYSE, familièrement appelé Wall Street, le Nasdaq, Bats, EDGX, etc.). Mais en 2014, il existe aussi quelque 40 « Dark Pools », ou bourses privées. Là, les transactions (analogues à celles réalisées à Wall Street) se font « sur invitation ».

**VOIP – Voice Over Internet Protocol** : protocole de transmission des messages vocaux sur l'Internet.

**VPN – Virtual Private Network** : réseau virtuel, privé mais légal. Circulant dans un « tunnel » crypté, les données sont « encapsulées » puis transmises de façon chiffrée – donc sécurisées. Seuls les ordinateurs situés aux deux bouts du tunnel accèdent aux données en clair (cryptage à l'entrée, décryptage à la sortie). D'où une grande (mais imparfaite) confidentialité.

**Zero Day** : exploitation le plus rapide possible, par un pirate, du « défaut dans la cuirasse » que peut présenter tout dispositif informatique. Auparavant non détectée ou non réparée, cette vulnérabilité est exploitée ou vendue « à chaud », lors même de sa découverte, sans attendre un seul jour, d'où son nom. Pour les pirates, la chasse au zero day est d'autant plus alléchante que les infrastructures critiques de la société de l'information sont pour la plupart fragiles ; et d'autant plus payante que, dans ladite société, tout le domaine du stratégique, sécurité nationale, économie, finance, sécurité sociale, repose désormais, à 100 % et définitivement, sur l'informatique.

# Préambule

> « Désormais dotés d'une dimension numérique, tous les crimes traditionnels deviennent plus dangereux, du fait d'une capacité croissante des criminels à cibler de nouvelles victimes. »
>
> Sanjay Virmani, directeur cybercrime d'Interpol – AFP, 2 mai 2014

Derrière le constant feu d'artifice des mille merveilles du high-tech et pour la première fois depuis un siècle, un écosystème nouveau bouleverse la planète en profondeur et chaque domaine de notre vie. Par « chaque domaine », nous entendons tout le commerce de l'humanité, toute sa technique et tous ses modes d'organisation, toute sa production industrielle et l'essentiel de sa consommation. Au début du XX$^{e}$ siècle, l'automobile fut « la machine qui a changé le monde ». Dès lors, se constitua un écosystème nouveau composé d'autoroutes et de raffineries, de stations d'essence et de fast-food. Le nouvel écosystème émergent et déjà dominant est fondé sur l'information digitale : son acquisition, son agrégation, son analyse, en masses toujours plus gigantesques ; là est, nous dit-on, la nouvelle source de richesses, le nouvel eldorado.

Songez : dans dix ans, 17 milliards de machines seront connectées !

Or fatalement, cet écosystème émergent aura sa face noire, sa dimension criminelle propre. Imaginer et pressentir cette dimension, repérer ses premiers symptômes et manifestations, ses premiers ravages dans le monde d'aujourd'hui, tel est l'objet de ce livre.

## Devant nous, sur la route…

Ce sera un livre de criminologie et tout, sauf un manuel technique sur la sécurité informatique proposant des rustines contre les risques d'intrusion. Conceptuel, cet ouvrage est consacré à pressentir le monde qui apparaît devant nous et les graves périls qu'engendre la « numérisation planétaire ».

Ce sera, nous l'espérons, un livre utile car, de fait, un monde nouveau émerge. On y voit d'abord survenir la seconde mort de Karl Marx : dans ce macrocosme nouveau, l'information (la superstructure) et la production (l'infrastructure) ne font plus qu'un. Les conditions sociales mêmes qui rendaient possibles le socialisme de Marx le rendent aujourd'hui impraticable : Amazon, Google, Facebook, Silicon Valley sont dans l'optique marxiste des OVNIS absolus ; et les envisager, ou vouloir les expliquer, selon les canons marxistes, n'a plus grand sens.

À l'issue du « grand basculement » qui s'amorce sous nos yeux, les fondements mêmes de notre société seront totalement et définitivement numériques.

Du « grand basculement », notamment criminel, qui s'opère aujourd'hui, une seule preuve suffit à ce stade : désormais, 70 % des dossiers d'enquêtes portant sur les trafics d'enfants (prostitution pédophile, vidéos pédopornographiques, etc.), montrent que la « transaction » s'est opérée en ligne, donc dans le cybermonde et *via* Internet*[1]. Selon les organismes internationaux spécialisés et le FBI, il y aurait mondialement, à chaque heure de l'année, quelque 750 000 pédophiles en ligne, chacun d'eux étant un prédateur potentiel et 40 000 sites de pédopornographie repérés et signalés.

Une fois ce grand basculement opéré, notre société reposera pleinement sur d'immenses architectures et plateformes informatiques ; celles des États, des organisations internationales et surtout celles des titans commerciaux ou sociétaux de l'Internet. Dès lors, nous vivrons tous et totalement dans l'économie de l'information où nous vivons déjà en partie.

Ce grand basculement du physique vers le numérique et, par conséquent, du crime physique vers le cybercrime*, n'est pas une hypothèse lointaine : sous nos yeux mêmes, il débute, il est là. Constamment et partout, sa face criminelle menace usagers et visiteurs du cybermonde : citoyens, administrations, industries, commerces, entreprises, etc. Nous allons en analyser les multiples formes : cyber-espionnage, fraudes identitaires et/ou financières sur Internet, attaques informatiques, faux et contrefaçons, racket, sabotages et trafics divers.

Plus encore, les responsables avertis prennent désormais conscience du fait que le cyberespace* est à coup sûr le nouveau lieu d'exercice global de la volonté de puissance, voire le théâtre d'une future « E-War », en français « cyberguerre »*.

Bref avant-goût de la menace :

– En juillet 2014, la BBC donne une idée du tsunami de dispositifs de piratage déferlant sur le cybermonde – et vraiment, les mots manquent pour donner au lecteur une idée de l'immensité du problème : 250 000 sortes de maliciels infestent quotidiennement l'informatique planétaire.

– À l'été 2013, Le FBI démantèle un cyber-gang (opérant depuis l'ex-URSS) ayant piraté les systèmes informatiques du Nasdaq, des entreprises JC Penney, Jet Blue Airways, Carrefour, 7-Eleven, PNC Bank, des filiales de Visa. Butin estimé : 300 millions de dollars. Or il existe déjà 200 à 300 de ces cyber-gangs dans l'ex-Bloc de l'Est, commettant tous des crimes d'autant plus ardus à réprimer qu'ils sont difficilement attribuables.

– L'énorme marché noir des logiciels pirates et autres outils cybercriminels brasse désormais des milliards de dollars par an. Il dispose à cet effet du Dark web, sur lequel nous reviendrons longuement.

– Parfois, des pannes géantes paralysent un cyber-géant (fin août 2013, le Nasdaq) ce qui expose un instant la vulnérabilité du système financier mondial. Mais par-delà la panne, quid en cas de sabotage ou de chantage criminel ? Aujourd'hui, nul officiel n'évoque clairement ce scénario plausible, ni ses éventuelles, et catastrophiques, conséquences.

– Ajoutons à cela le constant cyber-espionnage, d'abord opéré par le gouvernement des États-Unis (Prism, etc.), qui, sous couvert d'antiterrorisme, viole mondialement et systématiquement le secret des échanges personnels ou professionnels, dans le monde entier.

À l'avant-garde du grand basculement, concernés par les actions illégales que cette mutation engendre – mais souvent aussi complices de certaines d'entre elles – se trouvent les titans commerciaux ou sociétaux de l'Internet. Fin 2013, la capitalisation d'Amazon, qui a 210 millions de clients réguliers dans le monde, est de ± 135 milliards de dollars ; celle de Google, de ± 297 milliards de dollars ; celle de Facebook, de ± 94 milliards de dollars, etc.

S'intéresser à ces cyber-empires, c'est envisager toute l'économie et la finance du XXI$^{e}$ siècle, le Big Data* Business (commerce des gigadonnées). Chaque jour, ces cyber-compagnies, les gigaserveurs* du

commerce, du domaine sociétal ou de la finance s'internationalisent, se complexifient et deviennent indispensables à notre vie quotidienne. Or que veulent-elles exactement ? On le sait encore trop peu.

Titans, donc, mais fragiles, parfois semblables à de chatoyantes et éphémères bulles de savon. Exemple : le site REDDIT, qui, fin 2013, a doublé de taille en un an et compte 70 millions de visiteurs par mois – plus que le *New York Times* ou que Skype – mais fonctionne depuis un hangar avec 28 employés, à raison de 5 à 6 par tranche horaire.

Fragiles ou pas, ces géants de l'Internet sont les authentiques « puissances configuratrices » du monde émergent et, à ce titre, disposent bien sûr de leur idéologie propre. Comment ne l'auraient-ils pas ? Depuis deux siècles, l'industrie, le commerce, la finance, ont bien la leur : le libéralisme.

Notons d'ailleurs que le libéralisme préoccupe les criminologues sur sa grave myopie face au phénomène criminel. Or la Silicon Valley est idéologiquement bien plus extrême que le libéralisme classique, et « fonctionne » en ignorant délibérément les réalités criminelles du monde vrai, criminalité qu'il tient pour négligeable, voire risible. À de rares exceptions près, la « IT Crowd » (citoyens de la Silicon Valley) considère ainsi le crime comme un fait anodin : nombreux sont parmi eux les adeptes d'un libéralisme absolu, dit « libertarien », doctrine qui trouve un certain charme au crime organisé ; sa littérature en souligne les vertus et en vante les aspects positifs.

Nous ne noircissons pas le tableau et le sceptique peut, pour s'en convaincre, lire l'ahurissante bible libertarienne *Défendre les indéfendables : proxénètes, vendeurs d'héroïne, prostituées, maîtres chanteurs, faux-monnayeurs et autres boucs émissaires de notre société*[2].

L'opinion mondiale néglige cette idéologie libertaire et clairement destructrice du « vieux monde » – son maître-mot est *disruption* – ou alors, elle s'en moque. Nous montrerons plus loin à quel point cette ignorance est inquiétante, tant l'idéologie de la Silicon Valley affecte et configure la vie quotidienne des milliards d'individus connectés.

Nous exposerons donc cette *Silicon Valley ideology*, ou utopie digitale. Que des millions de geeks dans le monde croient dévotement en la capacité des ordinateurs à réaliser demain tout ce qu'entreprend aujourd'hui l'être humain, et bien mieux encore ouvre d'inquiétantes perspectives qu'il faut étudier, ce que nul criminologue n'a fait jusqu'ici.

Comme souvent, ces menaces sont d'autant plus sérieuses qu'elles sont insidieuses : on peut fréquenter le cybermonde des années durant et ne pas même imaginer ce que recèle sa face cachée. Ici, sonne toujours aussi juste et forte la parole de Frédéric Nietzsche dans *Ainsi parlait Zarathoustra* : « Ce sont les paroles les moins tapageuses qui apportent la tempête et les pensées qui mènent le monde viennent sur des pattes de colombes ».

Nous analyserons également de troubles connivences entre les autorités des États-Unis et les « Seigneurs de l'Internet » – libertaires certes, mais pas au point de refuser un petit service, quand la CIA le leur demande… Car d'évidence, ces rapports – allant jusqu'au symbiotique – de la Silicon Valley avec le Pentagone, la NSA* et la CIA, aboutissent aussi à des intrusions criminelles affectant la vie privée, de milliards d'internautes.

# Cybermonde : ce sur quoi nous bâtissons

Ce livre ne part pas de zéro : une bibliothèque entière a déjà été produite sur le sujet Internet – société de l'information – cybermonde – avenir de l'espèce humaine. Dans cette énorme base documentaire, nous prendrons comme guides deux récents ouvrages qui, à eux seuls, fournissent l'essentiel des références requises : *The new digital age – reshaping the future of people, nations and business* et *Cybersecurity and cyberwar – what everyone needs to know*[3].

Le premier est une ode aux lendemains qui chantent. Demain, demain matin peut-être, la connectivité universelle et éternelle ! Voici le gospel, ou techno-catéchisme, du nouvel âge digital. L'idéologie « solutionniste » à l'état pur : le high-tech est LA solution, partant de laquelle un avenir radieux est promis à nous-mêmes, à notre identité, à la citoyenneté en général, aux reportages des médias, aux États, aux révolutions, aux opérations antiterroristes ; aux conflits, combats et opérations extérieures, aux reconstructions post-ravages…

Ce livre de propagande pratique le classique « il-n'y-a-tout-simplement-pas-d'alternative ». Le Marché (ici, lire Silicon Valley) sait mieux que quiconque ce qu'il faut faire, et ce qu'on doit faire d'abord et avant tout, c'est de définir la connectivité à Internet tout à la fois comme une matière première et un droit de l'homme.

En prime, *The new digital age* déverse le prêche bienséant des Bonnes Causes, parfois proche du voyeurisme : « Au Pakistan, nous avons

rencontré un groupe de femmes attaquées à l'acide… »

Les notes en apprennent souvent beaucoup sur un livre. Dans celui-ci, il y en a 281, de Aadhaar (en hindi, programme visant à doter les 1,2 milliard d'Indiens de cartes d'identité high-tech, avec numéros à 12 chiffres, données biométriques sur une puce, etc.) à Zuma Jacob, président de l'Afrique du Sud. Là-dedans, 4 lignes de vagues allusions au crime. Rien sur la face noire de l'Internet.

Pas grand-chose sur le terrorisme sauf, au passage, une grosse bêtise : « Comme les terroristes inventent des méthodes nouvelles, les stratèges du contre-terrorisme s'adapteront à leur tour ». Or c'est l'inverse. Comme tous ceux qui vivent dans la clandestinité, les terroristes n'inventent quasiment rien et se bornent à réagir, s'il le faut vraiment. Auquel cas, ils font simplement et classiquement jouer à leur profit l'effet de déplacement.

Dans le second ouvrage, *Cybersecurity and cyberwar*… rien de proprement criminologique non plus. Dans un index de plus de 5 pages, pas une entrée sur le crime organisé, ni sur les cybercriminels. On est ici en plein entre-soi technologique ; les problèmes abordés sont entièrement techniques, l'« IT Crowd » officielle américaine se regarde le nombril.

# La voie criminologique

> « Ici, nous nous trouvons sans devanciers, et sans rien à quoi nous puissions nous tenir. Se contenter de mobiliser des variantes de ce qui a eu cours jusqu'ici, même en y joignant tous les modes de pensée que l'on aura acquis en suivant une procédure historisante, voilà qui ne fait pas bouger d'un pouce ».
>
> Martin Heidegger, *Apports à la philosophie*

Nous voici parvenus en *terra incognita* – « *Hic sunt dracones* » trouvait-on prudemment écrit sur les cartes médiévales censées dépeindre le centre de l'Afrique. Là, sur ces terres infrayées, il nous faut cesser d'évoquer, de comparer, de jauger mais bâtir et penser en criminologue.

Dès aujourd'hui, le système global de traitement automatisé des données constitue une superstructure mondiale. Le cyberespace représente un continent nouveau, un monde neuf. Or ces nouvelles technologies de

l'information et de la communication (NTIC) altèrent la façon qu'a la population de penser, de croire, de se comporter, d'apprendre. Toute la population : celle des honnêtes gens mais aussi, des malfaiteurs. Or comme toujours quand l'homme conquiert un nouvel espace, on ne tarde pas à y constater vols, fraudes, crimes, actions de propagande, truquages et mensonges, entre autres formes de déviance aux normes sociales. Il y a bel et bien un cybercrime, donc des cybercriminels : dès 2013, Interpol constate qu'à l'échelle mondiale, plus de 80 % de la criminalité en ligne émane de sociétés criminelles transfrontières.

Ce cybercrime est aujourd'hui le Graal pour tout malfaiteur. Jugeons-en :

– une totale dissociation du temps et de la distance offrant la capacité à commettre un crime à 10 000 km de distance (cyber-braquage),

– une jeunesse hypnotisée, facile à berner ou pirater, tant elle voit « le monde comme un ensemble d'applications ; leur propre monde comme une chaîne d'applications – voire parfois, comme une seule application étendue du berceau au tombeau »,

– des cerveaux cybercriminels, chefs de gangs ou têtes de réseaux, à l'impunité quasi garantie – aujourd'hui, seuls sont arrêtés de lointains comparses,

– des coûts limités pour des butins considérables,

– une méthodologie simple, exploitant deux fondamentaux : les faiblesses humaines (naïveté, etc.) et les vulnérabilités techniques (failles, etc.).

Dans la « sphère des évidences courantes », ou monde ambiant, de l'Internet, rien ne concerne le crime. On y parle parfois des effets du crime (attaques, intrusions…), jamais ou presque des criminels de chair et d'os, de qui ils sont ou de ce qu'ils font vraiment. Cet oubli est dramatique. Car s'il est une évidence, c'est la nécessité de nommer d'abord ce que l'on souhaite ensuite comprendre, puis traiter. Formidable est ainsi le discret pouvoir de la nomination : « Le nom fait faire connaissance… Nommer dévoile… Par la vertu de l'exhibition, les noms attestent leur souveraineté magistrale sur les choses », disait Martin Heidegger.

En médecine, par exemple, ne pas nommer une maladie grave condamne le patient ; en stratégie, encore, ne pas nommer précisément une menace condamne le plus souvent l'attaqué.

# Devanciers et précurseurs

> « C'était une de ses maximes qu'il fallait craindre les ennemis de loin, pour ne les plus craindre de près »,
> Bossuet, *Éloge funèbre du prince de Condé*

Ayant compris que la génération spontanée n'existe pas plus en criminologie qu'en biologie, certains chercheurs ont su s'extraire de cette « sphère des évidences courantes ». Ouverts au surgissement du réel, ils ont réussi à poser tôt des diagnostics informationnels lucides.

Le juriste et criminologue Gabriel Tarde a déjà, au XIX$^{e}$ siècle, dans son traité de philosophie pénale, décrit prophétiquement l'évolution de la mafia sicilienne : « En descendant de la montagne au littoral, elle change de caractère ; montagnarde et sauvage, elle est simplement brutale ; marine et urbanisée, elle est plus sanguinaire encore peut-être, mais surtout plus astucieuse et plus subtile ; son organisation se perfectionne, son outillage se renouvelle. Déjà *(les mafieux)* s'engagent toujours, soit implicitement, soit expressément dans leurs statuts, à pourvoir d'un avocat tout associé qui serait inculpé de quelque délit et à entretenir sa famille pendant la détention. Il s'est formé des sociétés criminelles, dernier avatar de la mafia… Faisant à leur gré la hausse et la baisse sur la place de Palerme, les adjudications de travaux publics ou de biens ecclésiastiques sécularisés peuvent être considérés comme une synthèse des deux brigandages ».

Voir devant, voir tôt, voir juste : de cela, la seule technique est encore incapable : elle ne peut toujours que prolonger des courbes. Pour l'instant, cette capacité prédictive appartient encore en propre à l'esprit humain, en mode philosophique. De fait, voyons avec quelle fulgurante précision, en trois phrases et dès la décennie 1940, un philosophe prévoit une société de l'information qui n'éclora qu'un demi-siècle plus tard : « Le poids croissant qu'acquièrent le calcul, la célérité et la revendication de ce qui se présente en masse… Le nombre et le calculable, c'est-à-dire tout ce qui est accessible à tout un chacun de la même façon… » ; la technique, qui « pousse tout en direction de la computation, de l'utilité, du dressage, de la maniabilité et de la régulation[4] ».

Mais venons-en au cybermonde et à ses prophètes.

Le lecteur lira avec profit les livres de Philip K. Dick, (bibliographie dans l'anglais original : www.philipkdick.com). Dès 1956, cet auteur imagine un monde où des voyants (*precogs*) prédisent des crimes, qu'on peut alors prévenir. De cette superbe et presciente nouvelle, Steven Spielberg tire en 2002 le film *Minority Report*.

Dès les années 1960 – cinquante ans avant les « retouches Photoshop » – Dick prévoit l'entrée de l'Amérique d'abord, puis du reste du monde, dans l'enfer de l'incertitude. Manipulée, falsifiée par de secrètes forces malfaisantes, la réalité ne mérite plus nulle confiance. Dans le cauchemar halluciné où rôde l'homme, le malaise a tout envahi ; il y survit par sa seule paranoïa. Auteur culte des geeks* d'aujourd'hui, Philip K. Dick est bien plus qu'un écrivain de science-fiction : un authentique devancier.

Ensuite, une lecture impérative, la seule à vrai dire qui concerne directement notre sujet, celle de *Who Owns The Future* de Jaron Lanier. Mieux encore que des phares, certains livres éclairent vers l'avant : authentiques projecteurs, ils illuminent l'avenir. Partant d'eux, des perspectives s'ouvrent, on peut penser devant, donc prévoir, puis prédire.

L'auteur avait repéré Lanier dès 2006, frappé par certaines de ses expressions, comme *digital maoism* ou *online collectivism*, parsemant un article lui aussi prophétique (<www.edge.org/conversation/digital-maoism-the-hazards-of-the-new-online-collectivism>). De fait et le premier des citoyens de la Silicon Valley, Lanier a vu que la « société de l'information », qui s'extasie pourtant sur la diversité – sans doute (pardon pour la jonglerie lacanienne) pour mieux faire diversion – avait à l'inverse la passion de l'uniformité et de la standardisation, ce que Hervé Juvin qualifie admirablement de « l'empire de l'Un », et un indépassable modèle, celui du banc de poissons. Le premier, Lanier a prévu le danger : celui de la caserne ou de la commune populaire digitales.

L'allure de Jaron Lanier est surprenante. À voir sa photo, on l'imaginerait plutôt jouant dans un groupe de reggae. On aurait tort : Lanier est un des grands pionniers de Silicon Valley, un parfait *insider*, mais ô combien lucide. D'une richesse, d'une densité exceptionnelles, son livre éclaire la perspective du cybermonde. On y voit l'avenir de l'économie de l'information. Autre motif d'estimer Lanier : sa méprisante détestation pour la pseudo-encyclopédie en ligne Wikipedia.

Tel est le cadre de l'ouvrage qui suit et tels sont les livres à lire pour l'apprécier pleinement. Première étape : Silicon Valley. S'agit-il vraiment,

comme le veut le cliché, d’un monde aimable et pacifiste, peuplé d’utopistes post-hippies ?

1. Tous les mots, expressions ou formules suivis d’un * figurent dans le glossaire, p. 13.

2. Walter Block, préface de Friedrich von Hayek, Les Belles Lettres, 1993.

3. Voir références et sources en fin de volume.

4. Martin Heidegger, *Apports à la philosophie* (*cf*. références).

## PREMIÈRE PARTIE

# CHAMP DE BATAILLE ET CADRE LARGE

Silicon Valley n'est pas qu'un simple lieu physique ; cette « vallée » n'est en rien un emplacement géographique anodin : c'est bien plutôt le réacteur ou la ruche d'où rayonne mondialement la cyber-économie, également nommée « économie-de-l'information ».

Là, naissent puis s'affirment les gigaserveurs qui sont les probables « puissances configuratrices » du monde à venir. Comprendre et connaître Silicon Valley est donc crucial : sa culture, ce qui s'y croit, ce qui s'y concocte. Il ne s'agit pas ici d'aduler ceci ou de condamner cela, mais de savoir.

# LE LIVRE DE LA CYBER-JUNGLE

Silicon Valley est d'abord le nid originel de l'utopie digitale qui, depuis les années 1950, a tour à tour agrégé à cette spiritualité orientale imprégnant San Francisco et la Bay Area depuis la décennie 1950 (George Gurdjieff, Allan Watts, etc.), d'abord la contre-culture hippie, puis la culture informatique et enfin un redoutable capitalisme.

Un pas préalable en arrière nous conduira d'abord sur la côte est des États-Unis, voici un demi-siècle, dans des campus en plein bouillonnement philosophico-théologique. Ce qui s'y déroulait nous convaincra que l'épopée Silicon Valley est tout sauf un cas exceptionnel, pour une Amérique de fait abonnée au prophétisme technicien et au mysticisme marchand.

En 1974, Raymond Ruyer narre cet épisode dans sa *Gnose de Princeton*. La gnose justement : quête spirituelle, voie mystique vers le royaume céleste… Seulement, aux États-Unis, c'est par la science et la technique qu'on espère accéder à l'esprit cosmique. Voici plus de quarante ans, l'un des savants gourous de Princeton cité par Ruyer présage déjà le rayonnement planétaire de Silicon Valley : « L'Amérique n'est impérialiste que malgré elle. C'est notre technique avancée qui absorbe malgré nous le reste du monde ». Mais comme c'est son « utopie digitale » qui définit et délimite au premier chef Silicon Valley, il faut remonter bien plus haut, car l'utopie accompagne dès l'origine toute l'histoire humaine. Surtout sous sa forme millénariste, celle qui annonce la fin du voyage et la sécurité du

terme, qui prône que l'humanité repartira un jour de zéro, qu'elle se reconstruira à partir d'une feuille blanche.

Cette utopie millénariste, que promet-elle ? Un jour, l'harmonie générale régnera et les gnostiques évoquent ici « le dimanche de l'Histoire », l'avènement de la restauration cosmique, le dernier état du monde. Toutes les races, toutes les espèces vivront en une immense concorde, dans la plénitude d'un monde restitué à sa maternelle et native harmonie. Plongé dans une parfaite béatitude, l'homme baignera dans la contemplation extatique et le fraternel partage des visions.

## « L'âge de cristal »

Voilà ce qu'annonce l'utopie digitale et voilà ce que croit la foule des geeks qui peuplent Silicon Valley. Mais ces obscurs et sans-grades du cybermonde ne sont pas seuls à boire cette grisante ambroisie : elle enivre aussi des cyber-milliardaires du net comme le P-DG d'Apple Steve Jobs, homme qui avait chevillé au corps la conviction de changer le monde et déclarait naguère publiquement vouloir « ébrécher l'univers ». Nous sommes à l'aube de « l'âge de cristal ». Les vieilles catégories de la politique et de l'économie ont vécu. Bientôt, viendra le grand bouleversement de la culture humaine. Quand cette mutation sera achevée, le monde sera transparent et la fluidité, quasi parfaite ; le risque disparaîtra, tout sera sous contrôle. L'abondance régnera, il suffira de se servir. Optimisés, les marchés seront hyperefficaces.

Actifs partout et tout le temps, les gigaserveurs parviendront à dompter la prosaïque réalité. La société de cristal sera dépourvue d'autorité centrale et d'impôts ; tout ou presque y sera accessible par presse-bouton – mieux, les machines se dirigeront par commande vocale ou par ondes cérébrales.

Si 2020, c'est demain, voyons maintenant après-demain, ou la semaine prochaine. Tentons de prévoir 2050. Écoutons les magiciens et enchanteurs du cybermonde à venir, tels qu'ils le prêchent dans les grands médias. En 2050, nous ne travaillerons quasiment plus, les robots remplaceront la main-d'œuvre humaine. Tout ou presque sera disponible, la sphère marchande aura basculé dans la quasi-gratuité. Robotisation, énergie : les innovations dans les technologies de l'information viendront par rafales, avec des gains de productivité exponentiels et quasi illimités. Les imprimantes 3D seront partout. L'énergie sera propre et inépuisable. La

communication sans-fil sera omniprésente et universelle. Grâce au high-tech, les campagnes répondront aisément et instantanément aux besoins des populations urbanisées. Les famines, alors ? Un cauchemar du passé.

Même, enfin, la télépathie ! Vers la moitié de ce présent siècle, des interfaces opéreront de cerveau à cerveau et transmettront directement des pensées, des impulsions ou sensations, traduites en signaux digitaux. Cela s'opérera de façon interactive, avec échanges possibles entre humains et machines. Sans autre médiation qu'Internet, le cerveau humain récepteur pourra par exemple exécuter toute tâche sans apprentissage, ni formation préalable.

Et la sécurité ? Entre cent splendides dispositifs, voici le « traqueur d'émotions ». Conçu dès les années 2020, il sera vers 2050 pleinement opérationnel dans les espaces publics à risque, aéroports, stades, métros, etc. Associant des capteurs, une vision informatisée par caméras et de puissants algorithmes, l'*emotion tracker* repérera les allures suspectes d'individus fortement émus ou agités, se pensant dissimulés dans la foule. Il n'y aura plus alors qu'à neutraliser ces suspects d'émotions dangereuses, voire homicides…

Le secret de cette incroyable révolution ? Les *collaborative commons*, le partage collaboratif rendu possible par l'interconnexion en un réseau mondial des « intelligences », à terme, de chacun des objets disponibles au monde. Ainsi prêche l'utopie digitale.

# Première composante : la gnose libertaire

Que cette utopie digitale irrigue, stimule et exalte un immense espace anarchique n'est pas une fantaisie issue de l'imagination de l'auteur. Au premier paragraphe de son introduction, le manifeste *Digital Age* le souligne en effet : « L'Internet est la plus vaste expérience anarchique de l'histoire ».

Car dès l'origine, l'idée libertaire est là. En 1984, en Californie bien sûr, se déroule la première conférence mondiale des hackers. Là, Steward Brand, éditeur du *Whole Earth Catalog* (la bible de la contre-culture) martèle « *Information wants to be free!* ». En 1992 cette fois, au Massachusetts Institute of Technology (Cambridge, Mass.), David Clark, pionnier de l'Internet, indique la juste voie idéologique : « Nous rejetons les

rois, les présidents et le vote. Nous croyons au consensus basique et au pouvoir du code *(code, au sens informatique)* ».

D'origine, les « valeurs de l'Internet » sont donc : « ouverture, coopération, innovation, gouvernance limitée et libre échange des idées ». Rien de plus normal, confirme un observateur attentif de cette scène : cette vision provient « du mélange, classique à l'époque, de libertés académiques et de mentalité hippie, avec une primauté de la connexion, du partage et de l'ouverture ».

La composante initiale du cocktail nommé « utopie numérique » est ainsi d'ordre politique et typiquement américain. C'est le courant libertarien qui, à un culte nietzschéen de la volonté de puissance, associe une double et exigeante passion pour la liberté individuelle et pour toutes les médiations électroniques. À quoi s'ajoute une vive horreur de l'État, toujours oppresseur, et des impôts : pour les libertariens, l'homme doit pouvoir quitter son pays aussi aisément qu'il divorce, ou qu'il abandonne son job chez un géant du net pour fonder sa propre startup.

Sergey Brin (cofondateur de Google), Jimmy Wales (fondateur de Wikipedia), Eric Raymond (théoricien de l'open source), John Perry Barlow (cofondateur de l'Electronic Frontier Foundation), Kevin Kelly (ancien directeur de la revue *Wired*), des financiers et hommes d'affaires comme Peter Thiel et Elon Musk, le courant du Technology Liberation Front, etc., se reconnaissent, à des titres divers, dans la doctrine libertarienne. Liberté pure et parfaite pour les entrepreneurs, pas de politiciens dans l'Internet ni dans le High-Tech, un monde en ligne hors d'atteinte des lois terrestres, échappant tant que possible à la réglementation de l'État : voilà ce que prône leur doctrine.

La société idéale des libertariens repose sur trois principes : ouverture totale, liberté absolue, démocratie radicale. Dans le domaine social, les avancées proviendront du progrès technologique ou de l'ingénierie ; le financement du social sera assuré par le capital de l'entreprise.

Attirante à première vue, l'utopie digitale prône quand même une dissolvante et discutable forme de liberté, celle du renard dans le poulailler.

Car derrière les grandes envolées, quelle est en fait la stratégie des géants du net ? Elle tient en un mot : *disruption* (perturbation ou interruption, en français). Usant de leurs gigaserveurs comme de *weapons of mass disruption*, les seigneurs de la Silicon Valley ont en effet ravagé, sous les coups de boutoir de leurs milliards, des industries et institutions

entières : la téléphonie, la musique, le cinéma, la télévision, la publicité, les médias ; sans oublier l'enseignement supérieur, la médecine, la monnaie. Et pendant ce temps-là, ils siphonnaient tranquillement Big Data et piétinaient au quotidien la vie privée de milliards d'internautes.

Or la liste de ces milliardaires-prédateurs s'accroît sans cesse : entre 2012 et 2013, dit la revue financière *Forbes*, l'introduction en Bourse des sites LinkedIn, Facebook, Twitter, ou d'applications comme WhatsApp, a suscité 12 nouveaux cyber-milliardaires en dollars.

# Seconde composante : la cyber-science-fiction

D'abord, ce second et bref retour en arrière.

C'est en 1955 que l'informaticien américain John McCarthy invente le terme d'« intelligence artificielle » (AI), une idée originale dont l'avenir est exprimé par les actuels visionnaires de la Bay Area en une formule : Singularité + robotique = AI.

En 1999, Ray Kurzweil publie *The Age of Spiritual Machines* ; il fonde ensuite l'utopiste courant de la Singularity* (2005, *The Singularity is near*) qui prédit qu'un jour (en 2014, Kurzweil voit cela advenir vers 2045) le réseau informatisé mondial constituera un seul ordinateur planétaire ; et qu'alors, cette giga-intelligence informatique outrepassera celle de l'homme. Notons que cela est loin d'être abstrait : depuis 2012, Kurzweil dirige le projet Google Brain, qui vise à faire, de ce qui fut un simple moteur de recherche, la première intelligence artificielle du XXI$^{e}$ siècle.

La science-fiction baigne et illumine certes la Singularité et le « Projet Transhumaniste ». Mais partout, sous-jacente et omniprésente, palpite l'idéologie libertarienne. Quand Lénine disait jadis, « le communisme, c'est les soviets plus l'électricité », on constate aujourd'hui que la Singularité, le Transhumanisme, c'est Ayn Rand (papesse de l'anarcho-capitalisme) plus les électrons. Pour tous ces libertariens doctrinaires, l'homme s'appartient à lui-même et est donc libre de se prendre pour terrain d'expérimentation. Le corps humain n'est pour eux qu'un logiciel reprogrammable et clonable, un prototype à perfectionner. La maladie, la vieillesse, ne sont pas fatales : domestiquons la vie à nos fins personnelles. Selon les progrès de la science, notre intelligence saura décider des « améliorations » à apporter à notre cerveau, à notre ADN ou à notre corps.

Toutes ces miraculeuses occurrences sont-elles seulement possibles ? Bien sûr, affirme l'utopie digitale, car voici qu'approche la « Convergence NBIC ». C'est-à-dire, les Nanotechnologies, la Biologie, l'Informatique plus les sciences Cognitives : en résumé, les sciences du cerveau plus l'intelligence artificielle, en interaction. Ainsi, l'homme est-il « NBIC-Perfectible », Demain par exemple, quand l'humanité aura pris son destin en main et qu'adviendra le grand croisement entre l'homme et des machines intelligentes, des applications pourront être téléchargées en direct dans le cerveau humain.

Déjà évoqué plus haut, Ray Kurzweil préside la Singularity University, où « bat le cœur de Silicon Valley » : c'est là où tout se divulgue, se prône et s'enseigne. Il faut ici redire que cette doctrine n'est pas celle d'une poignée d'illuminés : géant parmi les géants du net, Google partage et soutient, par exemple, la vision transhumaniste. Les cours de la Singularity University sont suivis par des icônes du show-biz (artistes, acteurs), des patrons de multinationales ou de startup californiennes. En outre, on croise dans cette singulière université toutes sortes de savants fous, de génies juvéniles et de futurologues exaltés. Là s'enseigne la contre-culture des années 2010 et ce n'est pas gratuit : 29 500 dollars pour dix semaines de cours.

Que sa vision l'emporte, et la Singularité promet monts et merveilles, car selon son slogan « le futur est meilleur que ce que vous croyez » : « En 2029, un bébé aura une chance sur deux de devenir immortel » (Kurzweil) ; dans l'avenir, les carburants se produiront à l'aide de micro-algues et les métaux précieux s'extrairont des astéroïdes, tandis que des plantes génétiquement modifiées produiront de la lumière. Plus généralement, ce ne seront sur terre et à disposition de tous, que robots sexuels, véhicules sans conducteurs et flux tendu systématique – tout et tout de suite.

Pour ces élus (au sens biblique) du néomonde à venir, les projets transhumanistes sont eux aussi des plus grandioses : ils vivront dans des villes-nations flottantes, installées sur d'immenses navires ou plateformes offshore, ancrés juste au-delà des eaux territoriales, hors d'atteinte des États rapaces et de leurs impôts confiscatoires.

Voués au high-tech, ces micro-États disposeront d'un système très perfectionné de formation/information en ligne ; les impôts y seront inconnus, on y paiera en cybermonnaies ; l'énergie y sera alternative et « propre », et les livraisons seront effectuées grâce à des drones. Ces

idéalistes et généreuses cités-laboratoires auront vocation à « nourrir les affamés, enrichir les pauvres, guérir les malades, régénérer les océans et l'atmosphère ». La mission même de Jésus plus l'écologie. Rien que ça.

Pour finir, voici le messianisme, le vrai : dans l'avenir toujours, Internet mutera en une intelligence artificielle ultra-sophistiquée, infiniment plus douée que n'importe quel homme isolé – et même, que tous les humains ensemble. L'informatique s'autodéterminera, se libérera de l'homme, deviendra une entité géante surnaturelle croissant de son propre et seul fait : ce sera l'avènement du cyber-messie. Le cybermonde l'aura emporté sur le monde physique.

Telles sont les visions – les chimères ? – qui traversent, enivrent et exaltent la Silicon Valley. Telle est l'immense arrogance prométhéenne qui habite cette vallée. Évidemment, chacun de ses habitants ne rêve pas de muter en un cyborg domicilié sur une plateforme offshore et payant en bitcoins* son écologique brouet tofu-vegan, mais ce mirobolant narratif est dans l'air qu'on y respire et de fait, il en inspire beaucoup.

Dès lors vient la question décisive : l'utopie digitale relève-t-elle de l'inspiration noble et sincère de visionnaires de génie ? Est-ce le trip de farfelus à l'esprit malmené par l'abus de substances psychoactives ? Ou alors, ne s'agirait-il que du chatoyant habillage de fort prosaïques prédations ? Pour les titans du net, la réponse est tout sauf claire.

Car, à aller au fond des choses et pour en rester aux seules entreprises de Silicon Valley, on constate qu'ils sont, pour ce qui les concerne, plus prudents que leurs propagandistes et thuriféraires, dans le registre des miracles à attendre de l'intelligence artificielle (AI). En août 2014, le très futuriste cyber-milliardaire Elon Musk diffuse ainsi un message d'alerte dans lequel il présente l'AI comme potentiellement « plus dangereuse que l'armement nucléaire » ; après avoir dit, dans un précédent message, redouter « un avenir à la Terminator ». À cette occasion, on apprend que Musk, Jeff Bezos (Amazon) et Mark Zuckerberg (Facebook) ont fondé une société de recherche sur l'intelligence artificielle, portant symboliquement le nom de « Vicarious » (expression complexe, mais généralement restrictive, de la langue juridique anglaise, signifiant « responsabilité dans l'exécution »)…

## DÉMONS ET MERVEILLES MÉDIATIQUES

Envisager le cadre large, c'est d'abord comprendre ce qu'est l'économie de l'information, ainsi nommée car, depuis la généralisation du cloud*, l'information y constitue plus que jamais le centre, avant d'en accaparer la totalité. En effet, les affaires qu'on y conduit impliquent toutes l'usage de logiciels sophistiqués et nourris d'information, les *software mediated technologies*.

Bouleversant l'économie comme la politique, ces technologies digitales provoquent la brutale mutation physique des métiers qu'elles détectent, assiègent, puis conquièrent. Pis encore, elles provoquent un séisme pour tout ce qui tient aux équations du pouvoir, précisément à la façon dont tout pouvoir se conquiert, se perd ou s'impose aux sociétés humaines.

À l'origine du séisme, les gigaserveurs voués, disent leurs concepteurs et propriétaires, à optimiser le monde, c'est-à-dire à le fluidifier, à l'ouvrir à la complexité. En matière de finance, c'est l'idée qu'exprime Lloyd Blankfein au *Times* de Londres, en novembre 2009 : « *We are doing God's work* ». S'il se montre provocateur, le P-DG de la banque Goldman Sachs n'est pas frappé de mégalomanie délirante, il est même au contraire fort logique : dans le monde de la finance, « accomplir le travail de Dieu », c'est optimiser tout ce qui s'achète, se dépense et s'échange sous le soleil. Les frictions, les blocages, voilà l'ennemi ! Dans le monde des réseaux d'échanges sociaux et du commerce, tel est également l'idéal des géants du net.

# Cyber-empires, les géants

Les quatre « super-géants » de l'Internet ont pour commun sobriquet « GAFA », pour Google, Apple, Facebook et Amazon. En avril 2014, la capitalisation boursière d'Apple est de 476 milliards de dollars ; celle de Google, de 371 milliards. Site marchand qui croît le plus vite au monde, Amazon a 209 millions de clients réguliers, et sa capitalisation dépasse celle de Boeing avec 148 milliards de dollars.

Facebook, lui, compte mondialement, 1,3 milliard d'usagers, dont 800 millions actifs, quasiment au quotidien ; pour l'année 2013, son chiffre d'affaires est de 7,9 milliards de dollars et son bénéfice, de 1,5 milliard de dollars.

Déjà en août 2013, Yahoo ! avait 196 millions de visiteurs uniques, Google, 192 millions, Microsoft, 179 millions et AOL, 117 millions. À l'été

2014, Twitter, qui n'était encore qu'une startup sept ans plus tôt, a 900 millions de comptes ouverts et 271 millions d'usagers mensuels actifs, tandis que 500 millions de « tweets » s'expédient chaque jour.

Désormais, ces géants tendent à se transformer en conglomérats, plus immenses et plus puissants encore. Au cours de ces dernières années, en effet, Google a acheté YouTube (vidéos en ligne), Motorola Mobile (téléphonie), Nest (domotique) et Waze (circulation) ; Facebook a acheté WhatsApp et Instagram (applications pour réseaux sociaux) ; Apple a acheté Beats Electronics (musique) et Microsoft a acheté Nokia (téléphonie).

Acquisitions à propos desquelles les analystes s'interrogent : sont-elles inspirées par une logique industrielle ou relèvent-elles de la mégalomanie et de l'idéologie « solutionniste », de l'idée que les cyber-empires, sont incroyablement intelligents et doués, savent et peuvent tout faire, notamment résoudre tous les problèmes du monde ? Le monde financier observe et attend.

# Cyber-empires, les titans

Après les entreprises géantes, voici les hommes qui les ont fondées ou les dirigent : ce sont les maîtres de l'économie numérique. En 2014, Silicon Valley compte une cinquantaine de milliardaires de cette nature et des millionnaires, par dizaines de milliers. Sur les milliardaires de moins de 40 ans, 10 dans le monde sont des tycoons du numérique. 20 % des Américains « riches » (dont la fortune est de 30 millions de dollars ou plus) vivent en Californie. Les fondateurs ou patrons de Google, Facebook, Amazon, Apple, etc., qui disposent de l'arme de la *disruption*, tendent à se considérer comme les nouveaux maîtres du monde. Il convient de noter que, pour ces cyber-milliardaires, Californiens de naissance ou d'adoption, les États-Unis ne valent pas mieux que les citoyens américains ordinaires : dans maintes des conférences qu'ils parrainent, l'Amérique est qualifiée de « Microsoft des nations », un géant bureaucratisé et dépassé, voué aux poubelles de l'histoire.

Le cas de Jeffrey Bezos, fondateur et patron d'Amazon, illustre parfaitement cette mentalité. Âgé de 50 ans, il est à la tête d'une fortune personnelle d'environ 30 milliards de dollars, la 19e du monde, selon le classement Forbes 2013. L'enfance de celui qu'un portraitiste dépeint

comme « un visionnaire, un innovateur, un destructeur » est classique pour qui est promis à un tel destin : « Ce fan de romans de science-fiction voulait construire des colonies humaines en orbite dans l'espace ». Son auteur favori d'alors ? Philip K. Dick. Aujourd'hui encore, Bezos fait tous les matins des exercices de gymnastique, persuadé qu'il est d'aller un jour dans l'espace.

Bezos, c'est aussi une ambition démesurée ; l'homme est brutalement inventif : « Pour la plupart d'entre nous, dit l'un de ses proches, créer la plus gigantesque librairie du monde aurait suffi. Mais son objectif est plus ambitieux : conquérir le monde ». Ce propriétaire de ce qui est aujourd'hui considéré comme « la boutique universelle » est aussi un vrai businessman : « Jeff est un capitaliste pur… Il ne raisonne que par chiffres… Le monde est son Hedge Fund ». Cet « ogre de la vente en ligne » ne laisse rien passer. « Comparé à lui, dit un collaborateur, le pire maniaque du contrôle (*control freak*) n'est qu'un hippie défoncé ». En politique, enfin, Bezos est libertarien, adepte du moins de gouvernement possible.

# Bezos et le monde de l'édition

Sans conteste, Bezos est aujourd'hui l'homme qui influe le plus sur l'avenir de la lecture, du livre et de la librairie. Une influence tout sauf bénigne : sur l'univers du livre en effet, Bezos pratique depuis l'origine, en bon disciple libéral-libertaire qu'il est de l'économiste Joseph Schumpeter, une fort efficace « destruction créative ». Amazon n'hésite jamais à « punir » les éditeurs qui ne se montrent pas assez souples lors de leurs négociations. Résultat : Amazon contrôle désormais environ les deux-tiers du marché mondial des livres numériques.

# Néomilliardaires et vieux médias

En 2013, Jeff Bezos rachète à titre personnel pour 250 millions de dollars le *Washington Post*, un de ces monuments de la presse-papier que les gigaserveurs ont largement contribué à couler. Des décennies durant, les grands quotidiens américains ont appartenu à de célèbres dynasties : les Bancroft (*Wall Street Journal*), les Chandler (*Los Angeles Times*), les Graham (*Washington Post*) et les Sulzberger (*New York Times*). Ces temps sont révolus. Place désormais à Jeff Bezos qui veut « réinventer le

journalisme », ou à Chris Hughes, l'un des fondateurs de Facebook, qui a racheté en juin 2012 un phare de la presse libérale (de gauche) aux États-Unis, *The New Republic*. Leur projet est de renforcer encore leur puissance en contrôlant le mieux possible la médiasphère, en achetant des journaux, mais aussi en finançant des bourses et des écoles de journalisme. Cela, d'abord et surtout pour échapper à des attaques médiatiques, toujours désagréables et potentiellement ruineuses.

Dernier investissement de Bezos-Amazon : le Cloud et le Big Data. Amazon web Services (AWS), la société qu'il a fondée à cet effet, a déjà, à la fin de l'année 2013, un chiffre d'affaires de 5 milliards de dollars et un taux de croissance, la même année, de + 90 %.

Voilà donc ce qu'est le type du titan du net. Les autres sont plus ou moins de la même trempe – sinon, parfois plus riches et avides. Côté hardware, Larry Ellison par exemple, le PDG d'Oracle, 5e fortune du monde, possède 25 % du capital de son entreprise et pèse 50 milliards de dollars. En 2013, Ellison a gagné près de 79 millions de dollars. De 2004 à 2012, 582 millions de dollars en tout. Eric Schmidt, président de Google, a gagné en 2013 100 millions de dollars en actions et 6 millions en cash.

Or, de façon surprenante, ces montants représentent cent fois plus que les bonus de Wall Street qui font hurler toutes les opinions publiques : fin 2012, le P-DG de Standard & Poors a reçu une prime de 251 000 dollars, et en 2013, Jamie Dimon (P-DG de la banque JP Morgan) a reçu 18,5 millions de dollars en action et 1,5 million en cash.

Le tsunami provoqué par ces géants du net menace la société américaine dans ses fondements mêmes. Une société sur laquelle, bourse et médias aidant, ils pèsent toujours plus lourd en compagnie des puissantes fortunes issues de l'ancienne économie. Conduite par deux prestigieux établissements académiques, Princeton et Northwestern University, l'étude intitulée « Testing theories of American politics: elites, interests groups and average citizens » établit que les États-Unis seraient en passe de devenir une oligarchie.

L'étude souligne que le système politique américain est toujours plus sous la coupe d'une élite économique. Le gouvernement n'y représente plus les intérêts de la majorité des citoyens mais ceux d'Américains riches et puissants. Le peuple influe peu sur les décisions politiques ; ce sont les élites économiques et les lobbies des affaires qui le font. Dans ce système, quand la majorité s'oppose aux 10 % les plus riches, elle perd. Quand une

majorité même large veut un changement politique, elle ne l'obtient pas. Le gouvernement cède le plus souvent aux pressions des grandes entreprises, du business et des syndicats professionnels.

## Milliardaires numériques : une certaine mégalomanie…

Ces cyber-milliardaires sont ambitieux et mégalomanes, mais quel épicier ne le serait pas si sa boutique comptait 200 millions de clients actifs et si son capital dépassait les 100 milliards de dollars ? Ils cultivent également une posture de démiurge passablement inquiétante. Pour s'en convaincre, imaginons un avenir où quelques dizaines d'entre eux contrôleraient les marchés les plus cruciaux. Dans ce monde, ils pèseront toujours plus sur des États peu ou prou cantonnés à la sphère du politique ou tentant de réguler, en courant lourdement derrière, des Goldman Sachs ou des Amazon. Après avoir chassé les politiciens du cybermonde, ces cyber-tycoons vont inévitablement envahir la sphère politique comme ils le tentent déjà. Il suffit pour s'en persuader de les entendre vanter leurs « dissolvants à dictatures », capables de déclencher à volonté des insurrections ou des révolutions. En citant comme exemple le catastrophique « Printemps arabe ».

## Miroir-aux-alouettes

Plus gênant encore est le mantra de l'utopie numérique qui tient en trois formules : « Optimiser le monde », « C'est gratuit » et « C'est sans risque ». En l'occurrence, on est pourtant loin du compte.

Optimisation ? À qui profitent l'optimisation et la « société ouverte » ? Au public ou aux consommateurs ? L'acte d'optimiser peut-il être défini comme une entreprise charitable ? Non : les gigaserveurs n'optimisent pas le monde, mais configurent le e-commerce et la e-finance au mieux de leurs propres intérêts.

Gratuité ? C'est la version numérique d'une escroquerie vieille comme le monde : l'illusoire promesse de créer quelque chose à partir de rien. La gratuité d'Internet au XXI$^{e}$ siècle est l'équivalent du don de verroteries aux sauvages, trois siècles plus tôt. Et aujourd'hui, le stratagème fonctionne

aussi bien qu'à l'époque. En Grande-Bretagne, une étude réalisée en août 2014 donne le prix à payer par un internaute pour bénéficier d'un web sans publicité : 140 euros par an. Cette même étude contient un sondage sur le nombre de Britanniques disposés à payer cette somme : 2 %, 98 % des sondés préférant un Internet gratuit. Et pourtant, celui qui soulève le rideau du gratuit constate vite qu'au service des géants du net, des sociétés de « marketing sur Internet » – en fait, des entreprises d'espionnage des vies privées – pillent et exploitent les données stockées dans le cloud, piétinant au passage ce qui tient à l'identité et la sécurité des usagers d'Internet.

Absence de risques ? Il s'agit d'une grave illusion dans le domaine de la cyber-finance – souvenons-nous de la crise des subprimes. Dans la plus totale impunité, des gigaserveurs financiers poussaient des consommateurs aveugles ou naïfs à acquérir des maisons bradées, à emprunter des sommes importantes sans limites, ni garanties, contreparties ou contrôles. Dans cette affaire, le risque réel a été totalement évacué. Grâce à des algorithmes truqués et à des agences de notation soudoyées, une cyber-finance a alors prétendu (s'est persuadée ?) que le risque ne la concernait plus. Or bien sûr, le risque était insupportablement réel et, *in fine*, Wall Street s'est effondré.

## Des manipulations sournoises

En juin 2014, les usagers de Facebook ont eu la surprise d'apprendre qu'en janvier 2012, 700 000 d'entre eux environ, anglophones, ont subi à leur insu une expérience de « contagion émotionnelle » : on les a utilisés comme cobayes, en manipulant leurs humeurs et émotions. Disposant d'une gigantesque masse de données sur ses quelque 800 millions d'utilisateurs quotidiens actifs, Facebook a « progressé » du passif à l'actif, en se transformant, le temps d'une expérience, en un inquiétant laboratoire du comportement humain. Il a fallu attendre le 17 juin 2014 pour que les usagers de Facebook découvrent le pot aux roses dans *Proceeds of the National Academy of Sciences*, revue officielle dans laquelle était froidement exposée cette expérimentation de manipulation psychologique visant à mesurer l'impact émotionnel propre de Facebook.

Ses utilisateurs ont-ils le moindre recours contre de telles pratiques ? Nullement : les conditions qu'ils doivent accepter s'ils veulent pouvoir s'inscrire sur la plateforme contiennent la disposition suivante : « Nous pouvons utiliser les informations que nous recevons à votre sujet pour des

opérations internes, dont le dépannage, l'analyse des données, les tests, la recherche et l'amélioration des services ».

Qu'a fait le service des analyses de données de Facebook ? Il a modifié les actualités à l'époque envoyées aux 689 000 cobayes ciblés, en accentuant leur *newsfeed*, soit en positif (c'est-à-dire en supprimant nombre de mauvaises nouvelles) soit en négatif (en effaçant les bonnes). Ensuite, Facebook a étudié les messages que, par la suite, les cobayes envoyaient à leurs contacts. Résultat de la manœuvre, le constat d'une évidence : les bonnes nouvelles mettent de bonne humeur. Et réciproquement. Bref : les émotions sont contagieuses. Tout ça pour ça ? Oui, mais reste la manipulation. Imaginons qu'elle prenne un tour idéologique ou religieux, les conséquences en seraient bien plus dramatiques…

# Idéalistes ou Tartuffes ?

Au cœur de l'idéalisme du cybermonde naissant – « ouverture, coopération, innovation, gouvernance limitée et libre échange des idées » – les valeurs de l'« open source community » sont les plus vénérées. Cette communauté réunit une phalange de programmeurs volontaires, travaillant en réseau sur Internet, à titre gracieux, pour concevoir des logiciels gratuits et supposés utiles au plus grand nombre, puis en améliorer l'architecture, l'aisance d'utilisation, y éliminer les bugs, etc. Or quoi de plus important que la sécurité des échanges et transactions sur Internet ? L'ayant compris, ces programmeurs volontaires inventent puis diffusent un logiciel de sécurisation libre et gratuit : Open SSL*.

Très vite, OpenSSL est adopté et utilisé gratuitement par Amazon, Cisco, Facebook, plus le FBI, le ministère des Finances du Canada, etc. Éclate en avril 2014 l'affaire HeartBleed, logiciel pirate qui infiltre justement le dispositif de cryptographie en open source OpenSSL et permet de récupérer de cruciales données de sécurité dans la mémoire d'un serveur * ou d'un usager. L'enquête révèle alors que le piratage d'OpenSSL date d'avril 2012 et a pour origine sa vétusté, son manque d'entretien.

Car de fait, l'architecture de ce logiciel n'a pas été revue/réécrite depuis 2004 ! Les rares volontaires entretenant OpenSSL disposent pour tout budget de 2 000 dollars (dons de particuliers), et travaillent sur OpenSSL pendant leurs temps de repos, sans salaire ni retraite, ni couverture sociale.

On comprend qu'ils puissent avoir d'autres tâches prioritaires et plus lucratives…

Les géants du net qui accumulent les milliards n'ont pas un dollar à consacrer à sécuriser OpenSSL, système omniprésent sur leurs gigaserveurs et présenté par eux comme parfaitement sûr. Tel est dans le concret, le respect qu'ils éprouvent pour les « valeurs fondamentales » de l'Internet. Leur désinvolture n'est pas moindre vis-à-vis de leurs propres employés, cadres et techniciens. En avril 2014, Apple, Google, Intel et Adobe systems sont collectivement condamnés à payer 324 millions de dollars à une coalition de 64 000 plaignants (*class action*), ingénieurs, programmeurs, etc. Ces quatre entreprises ont, en effet, étouffé entre eux la compétition du travail dans la Silicon Valley pour y contenir les salaires. L'acte les condamnant collectivement déplore une « obstruction à la mobilité de l'emploi et à la concurrence des compétences ». En termes clairs : un pacte secret existait par lequel elles s'interdisaient mutuellement de recruter des cadres ou techniciens les unes chez les autres.

On imagine l'immense emprise de Silicon Valley sur la foi américaine en la méritocratie mais ce jugement permet de constater que la réalité est plus sombre. Et certains médias en viennent à dénoncer dans l'affaire « une culture d'entreprise fondée sur le labeur de techno-serfs, plutôt bien payés mais d'évidence, exploités ». Car si « les seigneurs de la Vallée prétendent d'usage communier sous les deux espèces du Mérite et du Marché », ils se comportent plutôt comme, six siècles auparavant, les Grands Électeurs du Saint-Empire Romain Germanique : réseaux de complicité au sommet, administrateurs et conseillers communs, et discrètes manœuvres visant à exploiter les serfs. Conclusion d'un courageux journaliste : « Ceci est un exemple entre cent de la corruption de notre économie par cette intense concentration de pouvoir et d'argent ».

# Géants solides ?

Ultime remarque critique : les géants du net ont-ils vocation à durer ? Là encore, prudence car, comme le souligne un observateur avisé : « Dans la Silicon Valley, les fortunes se font et défont en fonction de la prochaine idée géniale ».

Nous vivons désormais dans un monde numérisé où les usagers consomment l'Internet sur des appareils mobiles, des tablettes, des

smartphones, etc. L'information récupérée est stockée en nuage dans des réseaux d'ordinateurs dont usent simultanément une multitude de sociétés. Or déjà, les géants d'hier peinent à s'adapter à ces nouvelles technologies de l'information et à la révolution de la mobilité : Hewlett-Packard, Cisco Systems, Intel, Oracle, Microsoft, Dell… Hier des géants du net mais demain ? Car, dans ce monde, les glissades sont brutales. « Pixmania, la chute éclair d'une étoile du web », titre *Le Figaro* en septembre 2013 : en 2011, cette icône de l'e-commerce dépasse le milliard d'euros de vente. Et prévoit même d'atteindre le milliard et demi d'euros en 2014. Sauf que, dès 2012, la société perd 48 millions d'euros et finit sa dégringolade en étant vendue à la casse, un an plus tard, à l'issue d'une fatale descente aux enfers.

## DEUXIÈME PARTIE

# LES CHAMPS DU CYBERCRIMINOGÈNE

On se souvient du fabuliste grec-phrygien Ésope et de son allégorie sur la langue, qu'il présentait comme étant à la fois la meilleure et la pire des choses. On pourrait parler d'un syndrome d'Ésope pour l'appliquer à quelques récentes découvertes socialement bienvenues mais potentiellement criminogènes. Des nouveautés qu'il serait impossible de vouloir proscrire – a-t-on banni le transport aérien après les attentats du 11 septembre ? – mais qu'il faut surveiller de près, du fait de leur grande capacité à servir de vecteur criminel.

Trois de ces inventions majeures symbolisent le mieux les évolutions de l'économie de l'information :

– la cybermonnaie bitcoin, dont l'origine est libérale-libertaire, mais dont le succès outrepasse les tracas qu'elle subit. Au point qu'elle, ou une autre analogue, pourrait un jour devenir la devise dont rêvent les jeunes générations, mondialisée, peu chère, discrète et sûre ;

– le Big Data, que certains voient devenir un levier économique sans égal depuis l'essor de la civilisation fondée sur le pétrole. Cet eldorado de données est présenté par un thuriféraire en ces termes : « Les données personnelles d'un individu sont bien plus précieuses que l'individu lui-même. Elles ne prennent aucune place, ne coûtent presque rien à entretenir ; elles sont éternelles, aisées à dupliquer et à transporter. Oui, ces données valent plus que leur poids en or, car elles ne pèsent rien : leur masse est nulle ».

– Les transactions boursières à haute fréquence* (*High Frequency Trading*, ci-après HFT), ou la possibilité d'accomplir des transactions financières massives, à la vitesse de la lumière. Mais aussi, l'énorme risque du dévoiement cybercriminel de ce que des prédateurs financiers shootés aux milliards de dollars nous présentent comme de simples mesures de « fluidification » ou « optimisation ».

## BITCOIN : ÉTOILE FILANTE, OU FUTUR ***CASH*** DE L'INTERNET ?

En une frappante formule, Carl Schmitt souligna naguère l'importance majeure de « la modestie secrète des commencements » : ce qui passe de prime abord inaperçu, le simple, l'inapparent ; tout ce qui, pourtant, nourrit

décisivement l'avenir. Soyons-y attentifs en abordant l'histoire des crypto-monnaies, singulièrement celle du bitcoin (sur les crypto-monnaies et toutes les rivales du bitcoin, voir l'annexe III).

# Une idée des libertariens

L'origine du bitcoin est idéologique. L'idée d'une cybermonnaie, ou devise électronique, fondée sur un code informatique open source, apparaît dans la décennie 2000, chez ces libertaires californiens partisans d'un capitalisme débridé et ennemis du gouvernement « à l'européenne », pléthorique et omniprésent. Encore qu'aux alentours de la Silicon Valley, l'idéal libertaire n'interdise pas forcément de côtoyer le Moloch étatique. Des esprits lucides soulignent ainsi que le logiciel de cryptage du bitcoin, le SHA 256 (Secure Hash Algorithm) a été créé par… La NSA (National Security Agency), puis remis au National Institute of Standards and Technology, pour usage public.

Cette open source est-elle donc totalement innocente ? Un expert travaillant sur les abus de la cyber-surveillance déclare ainsi en mai 2014 : « Je suis sûr que diverses agences travaillent à faire le lien entre les adresses bitcoin et l'identité réelle des utilisateurs, pour voir où va l'argent et à quoi il sert ». Inviolable ou pas, cette monnaie est à l'origine envisagée comme mondiale, anonyme, convertible (en devises réelles). Dans l'idée de ses anonymes concepteurs, elle échapperait à tout contrôle officiel, que ce soit celui d'un État ou d'une banque centrale. Uniquement échangée sur Internet, sa seule légalité reposerait sur son existence ; son prix, sur un strict mécanisme offre-demande.

Bitcoin apparaît en 2009. La légende voudrait qu'elle soit l'invention d'un informaticien japonais du nom de Satoshi Nakamoto, mais dans toute cette histoire, rien n'est sûr et Nakamoto ne serait qu'un pseudonyme. Dès l'origine, il est en revanche assuré que ne seront progressivement créées, en tout et pour tout, que 21 millions d'unités de bitcoin. Une quantité supposée garantir une attraction positive reposant sur l'offre et la demande, le système s'appuyant, lui, sur une architecture semblable à celle de l'Internet, donc capable de résister sans s'effondrer à toute attaque majeure sur l'un de ses points. Les bitcoins se négocient dans des *exchanges*, plateformes combinant les fonctions de bureau de change et de banque de dépôts, et une Fondation bitcoin (sans but lucratif) chapeaute le système et en regroupe tous les

grands opérateurs. Le tout fonctionne au jour le jour comme une monnaie « normale », à la double et remarquable exception que bitcoin ne s'appuie sur aucun État-nation, ou ensemble de type Union européenne pour l'euro, et que cette cybermonnaie n'a aucune contrepartie physique en billet de banque ou pièce de monnaie.

Les progrès sont rapides : le premier bitcoin s'échange pour 3 cents de dollar en janvier 2009 ; un an plus tard, cette même « pièce » « vaut » 29,57 dollars. En septembre 2012, on compte 35 000 transactions par jour dans le monde, 55 000 un an plus tard. La suite est plus agitée : début 2013, un bitcoin s'échange contre 13 dollars mais fin novembre de la même année contre 1 100 dollars, puis à 630 dollars en juillet 2014, non sans dramatiques péripéties entre-temps. Nouveau plongeon à 436 dollars, à la fin août 2014 (et ainsi de suite).

En mars 2014, 13 millions de bitcoins ont été créés depuis l'origine, et sont en circulation, pour une valeur mondiale (selon Fitch Ratings) de 6,75 milliards de dollars. Ce qui semble une somme énorme mais reste modeste si on la compare aux transactions quotidiennes en bitcoins pour 68 millions de dollars, de Paypal pour 492 millions de dollars et de Visa pour 19 milliards de dollars.

## Bitcoin ni sûr, ni stable

La première crise majeure de cette crypto-monnaie éclate en février 2014. Au début du mois, en effet, des pirates – qui restaient introuvables encore à l'été 2014 – neutralisent toutes les sécurités d'une des grandes plateformes d'échanges de bitcoins, Mt.Gox, implantée au Japon. Interdite de fonctionnement, celle-ci ne tarde pas à fermer – alors qu'à son apogée, fin 2013, elle brassait l'équivalent de six millions de dollars par jour en bitcoins. Volatilité ou chute libre ? Lors du krach, le bitcoin perd la moitié de sa valeur, d'environ 1 100 à 550 dollars avant de remonter à 630 dollars en juillet 2014.

Les pirates frappent fort : peu avant son effondrement, Mt.Gox subit par seconde environ 150 000 attaques en déni de service (DDoS*), qui laissent le système informatique de la plateforme ravagé. Mais quelles sommes les pirates pillent-ils au passage ? Il faudra du temps pour l'apprendre : au total, le vol porte finalement sur 660 000 bitcoins, soit quelque 5 % de tous ceux qui sont alors en circulation dans le monde et, à la valeur de fin février 2014

quand survient l'attaque, 310 millions de dollars environ. 100 000 bitcoins appartenaient à la plateforme Mt.Gox, le reste à ses clients qui perdent tout dans l'aventure.

Tout au long de cette première crise grave des cybermonnaies, on a beaucoup entendu parler de la victime, Mt.Gox, mais sans trop s'interroger sur ce que signifiait ce nom bizarre. Or le savoir en apprend beaucoup sur le fonctionnement du cybermonde. À l'origine, Mt.Gox est, en effet, la plateforme d'un jeu de rôle en ligne, Magic The Gathering Online eXchange, d'où l'abréviation en Mt.Gox. Une plateforme ensuite transformée en *exchange* pour bitcoins, brassant cyber-devises et dollars par dizaines de millions.

Après l'affaire Mt.Gox, d'autres *exchanges* sont braqués par des pirates. En mars 2014, par exemple, la plateforme canadienne Flexcoin se fait voler près de 600 000 dollars en bitcoins dans sa chambre forte virtuelle et se déclare en faillite.

## Un paradis pour malfaiteurs et anarchistes

Le cybermonde n'abrite pas que des libertariens, capitalistes dans l'âme, mais aussi des anarchistes d'extrême gauche, des hacktivistes* ouvertement « antifascistes » et hostiles au commerce, à l'industrie et à la finance privés qui poursuivent, notamment, les grandes banques de leur vindicte. Leur objectif n'est pas de fluidifier le système dans l'idée, finalement, de l'améliorer malgré lui, mais de faire échapper la finance à tout contrôle, de la désintégrer en rendant les transactions en bitcoins aussi parfaitement anonymes et intraçables que possible.

Sous le couvert du *dark web**, les hacktivistes ont créé plusieurs outils à finalités anarchistes tels que Dark Market, un site anonymisé de e-commerce en bitcoins, fonctionnant à l'origine sur Silk Road que nous analyserons plus loin ; Dark Wallet*, un portefeuille électronique en bitcoins accessible depuis un simple navigateur et configuré pour susciter à chaque usage une adresse furtive permettant de camoufler l'identité du bénéficiaire d'un transfert d'argent (ou sinon, de tout autre bien transférable) ; ou encore Darkcoin, évolution du bitcoin dont le code original contient, lui, ses propres lignes d'anonymisation, ce qui garantit donc le secret total des transactions et l'incognito des usagers. En mai 2014, un darkcoin s'échangeait contre

2,90 dollars. Aujourd'hui, des dizaines de plateformes négocient des darkcoins contre des bitcoins ou des dollars.

Point n'est besoin d'être un hacktivist pour utiliser les darkcoins : malfaiteurs, terroristes, porno-pédophiles, fraudeurs fiscaux, pirates, blanchisseurs d'argent sale et autres amateurs d'obscurité financière, ne s'en privent pas. Les libertariens, dont on ne sait s'ils sont ici naïfs ou lucides, nous présentent bitcoin et autres cybermonnaies comme l'arme des obscurs et des sans-grades, comme un bouclier de la cyber-finance au bénéfice des opprimés et des victimes des États. Selon les experts et les criminologues, c'est tout l'inverse : dès l'origine et aujourd'hui encore, les crypto-devises constituent plutôt une opportunité pour les prédateurs et les voyous de toute sorte.

Les cybermonnaies sont rapidement devenues le moyen idéal de payer des biens et services criminels ou illicites. Pour le prouver, juste un mot sur le supermarché de la drogue qu'est Silk Road, dont il sera question plus loin. Comment fonctionne ce site illicite ? Plus largement, comment acheter et vendre des stupéfiants, ou embaucher un tueur à gages, en restant hors d'atteinte de la police et de la justice ? Grâce à un usage combiné du logiciel « incassable » TOR* et des bitcoins, unique forme de paiement possible sur Silk Road. Ce n'est d'ailleurs pas par hasard si, lors de la fermeture de Silk Road par le FBI en mai 2014, bitcoin perd (encore une fois) la moitié de sa valeur…

Comment a fonctionné le précurseur de Silk Road, la plateforme Liberty reserve, sorte de Western Union mondiale du crime basée au Costa Rica, et démantelée par le FBI en mai 2013 ? Elle comptait déjà un million d'usagers dans 17 pays, la plupart en Espagne, aux États-Unis, au Nigeria, à Chypre et au Vietnam.

Grâce à des serveurs implantés en Suède, en Suisse et au Costa Rica, Liberty reserve expédiait de l'argent partout dans le monde, par voie électronique et sans trace (55 millions de transferts effectués). Des millions de dollars ou d'euros y circulaient chaque mois, entre de simples adresses courriel. Et pour un large éventail de transactions criminelles. Au fil des années, ont ainsi été repérés sur Liberty reserve des versements concernant des paris clandestins, des fraudes identitaires ou aux cartes de crédit, du piratage informatique, des escroqueries financières, de la pédopornographie, des trafics de stupéfiants, etc. Le tout, dans un anonymat garanti et, de 2006 à 2013, pour un chiffre d'affaires de 6 milliards de dollars.

D’autres malfaiteurs-internautes, russes ceux-là, se méfient des crypto-monnaies *made in America*. Pour eux, les anarchistes ou libertariens de Californie semblent trop proches de la NSA ou de la CIA pour que les systèmes « impénétrables » qu’ils proposent le soient totalement… et pour tout le monde. Le milieu cybercriminel de l’ex-bloc de l’Est propose donc ses propres cybermonnaies, elles réellement anonymes et intraçables.

La crypto-monnaie UAPS « First Commercial Bank », par exemple, apparaît fin 2012 sur un forum cybercriminel russe. Ses archives ne sont conservées que deux mois sur ses quatre plateformes opérationnelles, puis effacées du système. MUSD émerge en novembre 2013. Les « usagers » de cette plateforme et cyberdevise en même temps peuvent y acheter ou vendre ce qu’ils veulent, y promouvoir leurs propres produits, faire de la publicité, etc. À ce jour, la cybermonnaie MUSD s’échange contre des devises réelles, dollars, euros, etc., dans un seul bureau implanté à Kiev, Ukraine.

# Quand bitcoin sort de l’ombre…

On a cru dix fois la fin de bitcoin arrivée. Et encore en avril 2014, lorsque toutes les banques chinoises ont reçu l’ordre de rejeter tous les altcoins, dont bitcoin. Mais à chaque fois, l’alerte passée, bitcoin a rebondi, parfois vigoureusement. Une résurrection après chaque désastre. Et depuis le début de 2014, les signes positifs s’accumulent. En février, se crée à New York une bourse d’échange sérieuse de bitcoins, associant de grandes banques et d’importants régulateurs financiers privés. De grandes plateformes comme Coinbase, Circle, Blockchain.info et Payward s’intéressent désormais de près à l’industrie des crypto-devises,

Plus généralement, les grandes banques voient aujourd’hui bitcoin d’un œil moins antipathique ; elles imaginent même cette cryptomonnaie comme un nouveau système de paiement, moins cher que Western Union, Visa, etc. De son côté, une banque asiatique lance une application avec laquelle tout possesseur de Smartphone peut acheter des bitcoins, à partir de toutes les grandes devises mondiales. Un opérateur d’ATM invente, quant à lui, un système de petites annonces payables en bitcoins, et des distributeurs de bitcoins s’installent partout dans le monde : Texas, Nouveau-Mexique, État de Washington, Australie, Finlande, Allemagne, Slovaquie, Canada. Un

premier distributeur automatique à Bucarest en juillet 2008 et même à Las Vegas et Paris.

Au printemps 2014 « la folie bitcoin gagne Silicon Valley » : le capital-risque se lance dans les bitcoin-startup. Ces capital-risqueurs constatent en effet qu'il n'existe pas encore de moyen financier global et universel, de monnaie mondiale sûre et pratique, plaisant aux jeunes et répondant aux besoins d'une planète connectée et nomade. Après celui des hommes et des objets, l'Internet de l'argent reste à inventer ! Silicon Valley l'a flairé et prédit que c'est là qu'émergeront les futures entreprises milliardaires, les Google et Facebook de 2020.

Le bitcoin fait une importante percée au début de l'été 2014 quand Dell, 3e fabricant d'ordinateurs au monde (57 milliards de dollars de chiffre d'affaires annuel) accepte les règlements en bitcoin pour ses ventes en ligne, à partir du dispositif de paiement CoinBase – mais uniquement aux États-Unis ; même décision pour les grandes plateformes Expedia (voyages) et Overstock (commerce, soldes).

On apprend même en mai 2014 que, désormais considéré par le fisc comme un actif imposable, bitcoin est accepté par la Commission électorale fédérale des États-Unis, comme instrument pouvant concourir au financement des campagnes électorales. En juin 2014, le site VoxCoin est lancé pour recevoir et affecter les donations politiques en bitcoins.

L'ennui est que, dans cet élan collectif vers bitcoin, Silicon Valley et les hommes politiques américains cohabitent avec de multiples malfaiteurs ce qui, vu d'Europe et d'ailleurs, révèle une gênante et potentiellement dangereuse promiscuité. Qui, des « bons » ou des « mauvais » saura finalement chasser l'autre de cet outil monétaire ?

## BIG DATA : MINE D'OR, OU GRAAL DE L'ILLICITE ?

Au quotidien, le Cloud collecte une masse gigantesque d'informations. Comment exploiter et rentabiliser cet océan de données ? Tel est le projet de Big Data : mettre en place les systèmes informatisés de stockage et d'analyse (technologies et services) capables d'extraire, puis de transformer ces myriades de données éparses en *data pools* (bases documentaires), ordonnées, raisonnées et vendables ; ensuite, de repérer dans ces bases des

corrélations jusqu'alors inconnues, voire insoupçonnées, toujours à des fins commerciales. Et enfin, d'exploiter le plus pleinement possible ces bases et corrélations, aux plus proches limites du temps réel. Autrement dit de paramétrer l'existence des individus.

Ses thuriféraires disent l'avenir de Big Data incommensurable. Ce serait le nouvel « or noir ». À cette différence que, contrairement au pétrole, celui-ci est durablement et peut-être perpétuellement inépuisable, le volume des données produites doublant tous les deux ans.

## Une sévère crise d'hypertension numérique

Considérons les volumes de données produites par nos vies numériques et nos activités en lignes ; ajoutons-y le toujours plus intense trafic de l'Internet des objets (appareils entre eux, capteurs, etc.) : la « datafication » [mise en données, ou quantification] du monde s'opère donc aujourd'hui à toute vitesse, alors même que l'usage massif des processeurs et algorithmes transforme nos modes de représentation et d'action. Au cœur de ce maelström numérique, Big Data. Pour les experts, il fonctionne selon le principe des cinq V : Volume – Variété – Vitesse de traitement – Valeur des données – Vivacité du support.

Que le progrès technologique fasse simultanément exploser les cinq V et c'est le Boom. En effet, comme on l'a vu plus haut, toute l'économie du futur est fondée sur l'information, précisément sur l'exploitation par la publicité, le marketing et le management, des milliards de données recueillies au quotidien et constituant ensemble Big Data.

L'économie de l'information nécessite donc autant de Big Data que l'agriculture a besoin d'eau. Résultat : en 2010, le marché mondial du Big Data avoisinait les 3,2 milliards de dollars ; il sera de 17 milliards en 2015, soit 40 % de croissance annuelle.

## Big Data, version monts et merveilles

Les données sont un trésor : selon ses laudateurs, un Big Data intelligent permettra à la société humaine d'augmenter ses capacités de prévision, de localiser sans peine les individus, animaux, véhicules, etc. Grâce à Big Data, l'humanité saura aussi, mieux que naguère, prévenir les incendies et épidémies, l'exemple le plus fréquemment allégué étant que, plus

rapidement que les réseaux d'alerte des médecins, Google Flu Trends suit dans le monde la dissémination d'une épidémie de grippe. Enfin, Big Data permettra aux sociétés de mieux protéger leurs innombrables installations industrielles ou autres, et même de prévoir des événements comme les séismes et les crimes.

Notre avenir dépendrait ainsi de l'informatique cognitive (*cognitive computing*), née de l'exploitation conjuguée de systèmes gérant des données, et de logiciels chargés de les analyser. De même, existeront un jour (mais ce n'est pas encore le cas) des plateformes sachant « retrouver des aiguilles dans des meules de foin » numériques, comprenant les questions, raisonnant, résolvant des problèmes de mathématiques, sachant même décider.

La logique fondatrice du *cognitive computing* repose sur la constatation que tout ce qui nous entoure crée désormais toujours plus d'information : d'abord, les milliards de SMS, courriels, vidéos, tweets, commentaires publiés sur Internet, etc., émis par les individus ; ensuite, le foudroyant développement de l'Internet des objets : dès 2020, imaginons tout ce qui rayonnera de 40, voire 50 milliards de capteurs et d'objets connectés, entre autres les aéronefs, les véhicules, les radiateurs, les téléviseurs, les portes et portiques, les réfrigérateurs, les compteurs, les chariots de supermarchés, les montres…

Tout cela suscitera un immense marché de la « maintenance prédictive », voué à entretenir, régénérer, dépanner, cet univers de machines dont, affirment les adeptes de Big Data, l'humanité pourra pleinement tirer parti sans obstacles.

# Des millions d'emplois à fournir

Les grands agrégateurs de données (Amazon, Apple, Facebook, Google, Twitter, Yahoo !, etc.) ont donc le plus urgent besoin d'ingénieurs, de cadres et de techniciens bien formés. Savoir analyser, exploiter, optimiser et gérer le marketing de Big Data sera l'apanage de ces *data scientists* ou décrypteurs de données : autant de nouveaux et prestigieux métiers qu'il s'agit d'imaginer et de promouvoir. Pour la *Harvard Business Review*, la science des données – les comprendre, savoir les interpréter, leur donner un sens, où et comment les utiliser – est, en matière d'enseignement, « le secteur le plus sexy du monde ».

En la matière, les besoins sont énormes : dès 2015, il y aura mondialement 4,5 millions d'emplois à occuper, dont 1,9 million aux États-Unis, mais faute de compétences, un tiers seulement de ces emplois sera pourvu. Ainsi, toutes les grandes écoles mondiales en sciences, en management, etc., créent-elles en catastrophe des chaires, mastères etc., pour faire face à la ruée.

Fascinée, la France officielle lance un « Plan Big Data » à l'été 2014 : une coalition d'entreprises d'assurances lance un projet concernant les « jeunes conducteurs » et un autre, portant sur les « fraudes » ; Orange s'intéressera à une plateforme de collecte de données sur les objets connectés ; Gaz de France, Alstom, diverses PME montent un projet « villes intelligentes », visant à rassembler en masse des données sur l'énergie, les transports, etc.

# Big Data vous regarde : la version Big Brother

Début 2014, des journalistes du *Wall Street Journal* mènent une intéressante expérience. Partant d'un ordinateur neuf et de logiciels vierges, ils visitent les 50 sites les plus populaires de l'Internet (rassemblant 40 % de toutes les pages web visionnées par les Américains). À la suite de ces visites, ces journalistes retrouvent sur leur ordinateur 3 180 « cookies », aimable surnom de sinistres *tracking devices* (balises de traçage) déposées pour la plupart à leur insu. Un « flicage » soupçonné par les journalistes qui restent, cependant, ébahis par l'ampleur du phénomène. Le foisonnement de ce flicage systématique suscite de multiples questions : va-t-on vers une dictature du Big Data ? Voire vers un gouvernement par les chiffres de pans entiers de notre vie sociale ? Et où cette nouvelle économie de la quantification nous mène-t-elle ?

Que font, par ailleurs, les gouvernements et les géants du net des traces (opinions, goûts, états de santé) que nous laissons sur Internet ? Le consommateur est-il condamné à être ciblé et profilé ? Et surtout, quels risques proprement criminels renferme Big Data ?

De telles questions peuvent effrayer car, en matière de nocivité, force est de constater que certaines entreprises privées commencent à égaler la NSA. Par exemple, la société (américaine) Acxiom, spécialisée dans le *Consumer database marketing*, pratiquant le *behavioral targeting* (ciblage

comportemental) et désormais bien sûr, le *predictive targeting* (ciblage prédictif).

Acxiom possède 23 000 serveurs qui, chaque année, enregistrent et analysent 50 000 milliards (50 trillions) de données et transactions. À partir de ces immenses séries, elle constitue des dossiers sur la plupart des Américains – elle aurait fiché ainsi 75 % des consommateurs du pays. Chaque fiche de consommateur contient 3 000 à 5 000 *points* (éléments), tous récoltés à partir d'archives et données publiques ou privées, aisément accessibles : numéro de sécurité sociale, crédits en cours, casier judiciaire, etc.

Filiale d'Acxiom, la société ChoicePoint a, de son côté, agrégé 17 milliards de documents sur des individus et des entreprises, qu'elle vend à quelque 100 000 clients, dont 35 agences fédérales des États-Unis et 7 000 bureaux de police, de justice, etc., au niveau fédéral, local, ou de l'État. Mais la boulimie d'Acxiom & co. ne s'arrête pas là : elles traquent aussi les propriétés immobilières, les véhicules, votre consommation sur Internet, les réactions aux enquêtes de consommation. Plus, tout ce qui provient d'innombrables sources de cookies.

Combinées selon certains critères, les données détenues par ces sociétés fournissent aisément des catégories et des profils hautement sensibles. Par exemple, les militants de Greenpeace vivant près d'une centrale nucléaire, les musulmans pratiquants possédant une arme à feu, ou les habitants de tel quartier, ou les employés de telle entreprise dont le comportement est influencé par la Bible, etc. On peut aussi paramétrer ces bases de données pour qu'elles sélectionnent des catégories attentatoires à la vie privée (femme enceinte, personne âgée consultant des sites Internet consacrés au diabète, etc.).

Une surveillance d'autant plus inquiétante que l'instance professionnelle américaine Direct Marketing Association reconnaît discrètement qu'il n'est pas vraiment possible de se faire définitivement effacer (manœuvre d'*opt-out*) des bases de données de *data-brokers* comme Acxiom.

Acxiom a pour clients 12 des 15 principaux diffuseurs de cartes de paiement ; 7 des 10 principales banques de détail ; 8 des 10 grandes sociétés de médias/télécoms ; 9 des 10 grandes sociétés d'assurance sur les biens et la santé. Le gouvernement des États-Unis achète aussi régulièrement ses données comme à ses principaux concurrents, Experian et Epsilon.

# Big Data : le côté obscur de la force

Cette marchandisation des données est déjà peu rassurante, mais leur criminalisation l'est bien plus. La fraude identitaire en est un exemple. Sur ce marché illicite, les pépites se nomment des « Fullz* », dossiers individuels reconstitués comprenant nom, prénom, numéro de sécurité sociale, nom de jeune fille de la mère, etc. Tout ce qui, par exemple, permet de créer frauduleusement des dossiers d'obtention de cartes de paiement, ou de prêts personnels.

En 2013, une des grandes sociétés de Consumer database marketing, ci-dessus mentionnée, a vendu d'importants paquets de données à des pirates, qui en ont ensuite usé pour des escroqueries, des vols en ligne, du siphonage de comptes bancaires, etc. Il y a donc pire que d'espionner ses concitoyens : vendre les informations ainsi récoltées à des malfaiteurs ou encore, par cynisme, négligence ou défaut de contrôle, les laisser piller les data pools.

# Big Data ou Big Bidon ?

Distinguons le business du Big Data lui-même, lié à sa propre apparition et à son démarrage, de celui suscité par les technologies et entreprises ayant été créées dans ce domaine. Pour l'instant, Big Data n'est qu'une promesse pour l'économie et exploiter commercialement ses mirifiques capacités ne permet pas encore à une entreprise d'être rentable. En matière d'analyse, Big Data est plein d'opportunités mais celles-ci peinent à se transformer en commandes fermes d'entreprises ou d'administrations.

Les informations récoltées sur Internet sont-elles exploitées « au profit des consommateurs », comme le prétendent les entreprises de marketing ? Non. Publicités ciblées le plus précisément possible, harcèlement des consommateurs et usagers en témoignent. Certains experts en viennent même à dénier au Big Data tout réel intérêt dans le domaine de la vente. Car que fait le *consumer data marketing* ? Il expédie au consommateur des publicités pour des produits qu'il a déjà achetés, ce qui s'appelle prolonger une courbe ; ou encore, un algorithme de marketing crée un lien grossier entre deux achats et suppose que, comme vous avez aimé A et B, vous adorerez C. Ce qui ne s'appelle pas du marketing, mais plus simplement du *wishful thinking* : Big Bata saute à la conclusion et surtout décide formellement, à partir de faits ambigus. Que signifie, en effet, consulter un

site donnant des recettes de bombes artisanales ? Qui se trouve de l'autre côté de l'écran ? Un dangereux terroriste ? Des gamins se donnant des frissons ? Un étudiant en chimie ? Un artificier désireux d'élargir ses connaissances ?

Bref, concluent les critiques, Big Data opère à l'aveuglette. Et cela commence à se savoir puisqu'en juillet 2014, le *Financial Times* publie un article explosif sur « la folie des grandeurs du Big data » (*Google catches cold as debate over Big Data Hubris rages*).

En 2008, en effet, Google lance un dispositif en ligne de dépistage de la grippe nommé Google Flu Trends (GFT). À partir des recherches sur le mot « grippe » opérées sur cette plateforme, et après analyse informatisée, les promoteurs de GFT estiment qu'on peut prévoir les épidémies – au pire, les détecter à leur tout début. La démarche est publicitairement géniale et socialement admirable : l'Internet comme outil de santé ! Mais six années plus tard, GFT est plutôt donné en exemple des limites et faiblesses de Big Data, notamment dans une étude de la revue *Science* de mars 2014, intitulée « *The parable of Google flu – traps in Big Data Analysis »*. Réalisée par des scientifiques de Harvard et de Northwestern University, elle nous apprend en effet que, depuis son lancement, GFT se trompe souvent : saison 2012-2013 – GFT annonce que 10,6 % de la population américaine est en train d'attraper la grippe mais il n'y aura finalement que 6,1 % de grippés aux États-Unis, cette saison-là ; saison 2013-2014 – GFT affine ses algorithmes, peaufine ses logiciels et « tape » quand même 30 % trop haut.

Conclusion de l'étude de *Science* : les données rassemblées par GFT trahissent plus des inquiétudes que des symptômes et reflètent sans doute plus d'auto-intoxication que de ressenti fébrile, ce qui n'a, pour l'instant, aucune valeur prédictive. Les prévisions et analyses faites par les réseaux de praticiens du US Center for Diseases Control sont bien plus précises et efficaces, même s'il faut deux semaines pour obtenir des résultats définitifs.

Erreurs de jeunesse de Google Flu Trends ? Défauts structurels ? Impossible de trancher aujourd'hui, l'aventure Big Data débutant à peine. Mais lorsque nous aborderons le domaine voisin de la prédiction policière, nous verrons qu'une grande prudence est de mise.

## LES TRANSACTIONS À HAUTE FRÉQUENCE (HFT, POUR ***HIGH FREQUENCY TRADING****)

Ce qui suit n'est pas une étude sur les HFT, ni sur le risque criminel qu'elles présentent. D'autres ont déjà abordé le sujet avec autorité, à commencer par Jean-François Gayraud dans son *Nouveau Capitalisme Criminel*[1]. Nous explorons ici un domaine plus étroit, cantonné à l'univers numérique et aux grands acteurs financiers qui y opèrent. Ces acteurs sont des banques géantes ou des milliardaires, agissant aux limites extrêmes de la fraude ou du délit d'initié ; des entités ou individus ultrarapides et brillants confrontés à des bureaucrates lents, lourds et perdus dans un « brouillard de la finance » plus impénétrable encore que celui de la guerre.

Ces banques géantes, nul ne les ignore car il n'est pas de semaine sans que certaines d'entre elles ne soient sanctionnées par des amendes de plusieurs milliards de dollars, pour des infractions financières allant de la banale acrobatie de marché à des collusions avec des mafias.

Naguère encore, ces banques, souvent centenaires et authentiques monuments de dignité financière, étaient fort réputées. Comment ont-elles pu autant s'égarer ? La réponse est dans leur informatisation. À cause de ce processus, elles se sont transformées en d'immenses réseaux planétaires et ont métamorphosé la finance mondiale en un casino géant, fondé sur les profits de produits ésotériques et de martingales numériques. Une mutation car, si l'initial (et légitime) objet du processus était d'optimiser la circulation des informations et ordres divers, la finance de l'information a surtout permis de frauder plus et mieux.

Nichés aujourd'hui – et un peu plus chaque jour – au cœur de toutes les entreprises humaines, des cyber-outils toujours plus complexes manipulent à toute vitesse l'argent stocké entre serveurs et réseaux. La cyber-finance *criminelle* est le dévoiement de ce processus d'optimisation. Dans ce système, l'informatisation est cruciale : à l'échelle de Madoff, celle des dollars pillés par milliards, l'escroquerie est impossible sans gigaserveurs et Big Data qui, seuls, permettent d'amplifier et de démultiplier une corruption et des fraudes, sinon forcément médiocres. Pourquoi ? Nul – et surtout pas les régulateurs étatiques – ne sait plus aujourd'hui ce qu'il advient des milliards une fois introduits dans le circuit, par où ils passent et où ils atterrissent. Telle est aujourd'hui la seule forme de fraude financière possible et brutalement lucrative.

Florissante et hyperactive, la cyber-finance dévoyée est, à ce jour, quasiment impunie. Les banques géantes et autres prédateurs s'amusent des milliards de dollars d'amende qui pleuvent sur eux et qui, s'ils

impressionnent l'opinion, ne représentent en fin de compte qu'une minime partie de leurs profits.

Comment en est-on arrivé là ? Le problème majeur du cybermonde est son défaut d'un « code » de conduite global, sans lequel les sanctions actuelles resteront inefficaces. À cause de cette lacune, demain risque d'être pire encore en matière de cyber-finance et l'avenir proche pourrait bien ressembler à ceci : avec des pouvoirs et fortunes toujours plus concentrés, des prédateurs conduisent leurs raids depuis des forteresses virtuelles ultra-sécurisées, en usant de dispositifs financiers opaques, incompréhensibles pour les États et les régulateurs.

# HFT : une escroquerie rapide comme la lumière ?

Grâce à un système *ad hoc*, l'objectif du HFT est de détecter les mouvements imminents d'une bourse afin d'exploiter ces amorces de fluctuations à son propre profit. Les transactions à haute fréquence sont un dispositif automatisé de plateformes boursières associant des algorithmes sophistiqués à des serveurs de grande puissance opérant à la nanoseconde près. Sur des centaines de kilomètres parfois, des tunnels rigoureusement horizontaux creusés entre bourses et plateformes spécialisées sont équipés de câbles en fibres optiques d'une qualité optimale, pour envoyer et recevoir un signal le plus rapidement possible. Ici, la milliseconde qui permet de prévoir rapporte une fortune.

Au printemps 2014, on apprend ainsi que, sur trois ans, la société américaine de *trading* à haute fréquence VirtuFinancial a réalisé des profits dans 1 237 des 1 238 séances de la Bourse où elle est intervenue. Une seule perte en trois ans : on voit bien qu'il s'agit plutôt d'une martingale que d'opérations boursières ordinaires. Ajoutons-y les microfraudes baptisées « front-running », « spoofing », « quote stuffing » ou « subpenny », opérées au quotidien, en quelques millièmes de secondes, sur d'énormes volumes d'actions. Avec comme conséquences que, sous les coups de boutoir des opérateurs de HFT, les grandes bourses de valeurs, menacées de mort, ont dû éclater en de multiples plateformes d'échanges spécialisées, de taille plus réduite, enclenchant ainsi un maelström financier toujours plus complexe et finalement incontrôlable : les flux financiers allant toujours plus vite et on ne sait où, les investisseurs sont désormais incapables de savoir ce qu'on fait de

leur argent, où il se trouve et par où il est passé. Cela, seul l'opérateur HFT le sait – peut-être.

Les acteurs du HFT prétendent, au contraire, qu'ils assurent la liquidité des transactions, que grâce à eux, les marchés sont plus fluides et rapides, et les transactions moins onéreuses. Mais pour nombre d'experts et de régulateurs, c'est plutôt de volatilité qu'il faut parler. Pourquoi ? La liquidité que les HFT se vantent d'apporter au système boursier est illusoire car, en cas de drame, crash ou guerre, cette liquidité s'évapore et tout se fige. On en veut pour preuve que, lors de la brève mais violente chute de Wall Street (« *flash crash* » du 6 mai 2010) où le prix des actions plonge de 600 points en dix minutes, les sociétés de HFT ont sur le champ cessé d'échanger, ce qui a encore aggravé le plongeon.

Par ailleurs, les HFT anesthésient le système ou le rendent autiste. Au point que 60 à 70 % des variations de prix des actions sont totalement déconnectés des événements advenant simultanément dans le monde réel. Enfin, de 2007 à 2014, le coût du *trading* boursier est resté sensiblement le même aux États-Unis alors que, grâce au HFT, il aurait dû baisser.

Cela n'a pas empêché Goldman Sachs, Royal Bank of Scotland, UBS, Deutsche Bank et JP Morgan, pour n'en citer que quelques-uns, d'investir des milliards dans ces systèmes informatiques et ces algorithmes. Même les fonds de pension qui, dans la sphère financière, passent pour des parangons de prudence et de patience, jouent désormais au HFT. On assiste ainsi à une « guerre totale entre sociétés de HFT dans un contexte de chute de leurs revenus ». Une course à la vitesse si folle qu'aux États-Unis, le FBI, le ministère américain de la Justice et la Securities and Exchanges Commission en viennent à parler de système pervers.

Possédant les algorithmes les plus sophistiqués, les plateformes boursières électroniques (initiant désormais la moitié des transactions opérées aux États-Unis) faussent les marchés financiers et pénalisent les autres investisseurs. Réagissant plus vite que tout autre, elles précèdent et détectent les intentions des investisseurs de base, puis les grugent. La complexité du système (la forme) masque les opérations elles-mêmes (le fond). Un régulateur dépassé affirme ainsi : « Si c'est tellement compliqué, c'est incompréhensible, donc impossible à interroger ou à critiquer ». D'évidence, le HFT offre ainsi de fascinantes opportunités à tous les corrupteurs et blanchisseurs d'argent sale sensibles au high-tech. Et laisse le monde boursier face à une menace majeure : celle d'un nouveau *flash crash*,

d'origine terroriste ou criminelle, semblable au brutal effondrement de Wall Street du 6 mai 2010.

Ce risque n'est pas illusoire : chaque jour, des experts spécialisés détectent des micro-tsunamis par centaines, qui durent chacun moins d'une seconde pendant laquelle des actions s'effondrent et se reprennent tout aussitôt. À ces préoccupations technologiques s'ajoutent désormais d'autres, criminelles cette fois : en juin 2014, un important trader HFT est ainsi victime d'une cyberattaque sophistiquée. C'est la première du genre à Wall Street. Le nom de la victime n'est pas divulgué mais des fuites permettent d'estimer qu'il s'agit vraisemblablement de Citadel ou de Renaissance, les deux grands du HFT. Deux mois durant, un subtil sabotage a ralenti l'exécution des ordres, tandis qu'un maliciel, infiltré par le truchement d'un courriel d'apparence anodine, a pillé les données stratégiques de la société : ses protocoles et priorités, ses intentions, bref ses secrets d'entreprise.

## *CYBERMAN* : L'HOMME NUMÉRIQUE, SA VIE, SON ŒUVRE

Trois milliards d'humains accèdent désormais quotidiennement au cybermonde. Pour le meilleur ou pour le pire comme un criminologue doit l'envisager, s'il est adepte du décèlement précoce des dangers et menaces. Plongé dans l'univers cybernétique, le plus souvent sans imaginer même les périls qu'il renferme, le « cyberman » dont on commence à distinguer la silhouette promet d'être un étrange citoyen. Il n'est bien sûr pas question de prôner ici le retour à la lampe à pétrole ni à la plume sergent-major, mais simplement d'observer dans quel état ce « cyberman » émerge pour imaginer à quels risques criminels il sera confronté et les outils dont il disposera pour les affronter.

Philip K. Dick, voici cinquante ans et le tout premier, a, avec une étonnante précision, prévu l'homme-appli, docile zombie des puissances du cybermonde. La réalité a rejoint ce modèle avec, par exemple, un certain « Chris Dancy, l'homme le plus connecté du monde » comme l'a baptisé *Paris Match*. De sa propre initiative – nul de l'y contraint – Chris Dancy est « suivi, traqué, chronométré par des dizaines de caméras et d'appareils portatifs qu'il n'a cessé d'accumuler an cours des cinq dernières années. Il se rêve en homme augmenté. Avec un objectif ultime : hacker son propre cerveau ». Pour lui « l'informatique pénètre notre corps pour allonger nos

vies ». Clairement, on est ici en pleine utopie digitale, versant transhumaniste.

Chez Dancy et dans sa voiture, 13 dispositifs mesurent le bruit, la qualité de l'air et la température, la pression atmosphérique et l'humidité, détectent tous les mouvements, mesurent les ondes Wi-Fi et combattent leurs effets néfastes, surveillent l'activité de ses chiens, enregistrent en temps réel, en vidéo, l'activité de sa maison, règlent les températures, détectent le gaz carbone, mesurent la qualité de son sommeil, l'acuité de son attention dans sa voiture, indiquent les objets connectés proches et règlent ses haut-parleurs… Chris Dancy a institué et perfectionné sa propre NSA à lui tout seul et est devenu le superflic de lui-même.

Quand « Cyberman » fera des études supérieures, il devra se choisir un camarade de chambre. Par affinité ? De façon aléatoire ? Non : un algorithme l'y aidera. Les logiciels StarRez et RoomSync sont déjà prévus pour satisfaire les (politiquement corrects) desiderata de chacun en la matière.

Si « Cyberman » veut choyer son animal de compagnie, le nouveau logiciel Bistro se révèle indispensable. Cet outil de reconnaissance faciale pour chat comprend une mangeoire équipée d'une caméra (qui identifie tout animal) et une paillasse truffée de capteurs (qui pèsent la mangeoire et le chat, pour constater ce qu'il a ingéré). Pour 299 dollars, Bistro permet, non seulement de voir en direct son chat manger à Paris, depuis une chambre d'hôtel de Valparaiso, mais il archive (avec tableaux, graphiques, etc.) toute la vie de l'animal, puis communique l'ensemble sur un smartphone.

Bistro comprend un dispositif d'alarme en cas de problème, et donne des conseils pour mieux alimenter l'animal. Tout cela en attendant que les progrès du high-tech donnent à « Cyberman » la capacité de s'offrir un robot-chat. Mais alors, que se passera-t-il ? Pour le savoir, il suffit de lire *Do androids dream of electric sheep* de Philip K. Dick.

Si, à présent, « Cyberman » s'inquiète de sa partenaire et se demande si elle est fidèle, la société mSpy l'aide à le savoir grâce à son logiciel mCouple. L'installer sur le smartphone de la partenaire (en le lui disant ou pas) permet, en effet, d'y récupérer tout ce qu'on veut : messages, courriels, échanges sur les réseaux sociaux, photos, vidéos, etc. Mieux encore, mCouple, permet aussi d'enregistrer toutes les conversations téléphoniques et de localiser le téléphone du partenaire au mètre près. La société mSpy

vend aussi des logiciels pour parents désireux de surveiller leurs enfants, ou pour patrons voulant espionner leur personnel…

Malheureusement, les dispositifs décrits ci-dessus sont riches en virtualités criminelles, comme affamer ou gaver le chat d'un ancien partenaire par piratage ; ou installer dans la même chambre un militant des droits civiques et un membre actif du Ku Klux Klan de l'Alabama ; ou encore provoquer la rupture du jaloux convulsif d'avec une innocente.

***

Après cet indispensable « champ préalable d'inspection » (*cf*. Annexe I) – d'où vient le phénomène de la criminalité numérique ? Où est-il apparu ? Qui a-t-il affecté depuis son origine et qui inquiète-t-il aujourd'hui ? Où, comment et pourquoi, se répand-il dans le monde ? – nous pouvons aborder la partie proprement criminologique de cette étude.

1. Odile Jacob, 2014.

## TROISIÈME PARTIE

# MÉANDRES ET PERCÉES DU CYBERCRIME

Quelques chiffres pour commencer, même s'ils sont pour la plupart périmés dès qu'ils sont publiés : collectés et vérifiés du début 2013 à l'été 2014, ils ont depuis augmenté, voire explosé. Néanmoins, ils donnent l'idée, même grossière, d'un cybermonde de l'illicite ayant potentiellement atteint la dimension d'un univers.

# UNE CYBER-SCÈNE DE CRIME ILLIMITÉE OU PRESQUE

En 1930 – dans des circonstances absolument différentes – Mao Zedong prononçait sa célèbre déclaration stratégique : « une étincelle peut mettre le feu à toute la plaine ». Difficile d'imaginer formule plus pertinente pour décrire la foudroyante progression des nouvelles technologies de l'information et de la communication : il y a vingt ans (hier, en termes historiques) rien, ou presque. Et aujourd'hui : trois milliards d'humains connectés à l'ensemble Internet – logiciels – systèmes de communication mobiles.

De 1973 à 2013, la croissance de l'Internet a été exponentielle. Il a, en effet, crû un million de fois, en nombre de machines, en rapidité du réseau et en capacité de mémoire disponible. En 2013 (dernière année complète), on compte 759 millions de sites recensés, dont 510 millions sont actifs (le premier site web fut créé en 1991). Rien que pour l'année 2013, on compte 103 millions de sites nouveaux et 328 millions de noms de domaines enregistrés. Au total, 1,193 milliard de noms de domaines sont enregistrés.

Fin 2013, il existait environ 30 trillions de pages web, dont 14,3 trillions accessibles, soit quatorze mille milliards virgule trois de pages web consultables (un trillion = 1 000 milliards). Au même moment, le nombre des octets (la plus petite unité de données en informatique, *byte* en anglais) composant l'ensemble de l'Internet – les briques ayant servi à construire l'édifice – est au total estimé à 1 suivi de 24 zéros. De 2000 à 2012, le nombre des êtres humains connectés à Internet était passé de 350 millions à 2,4 milliards. Fin 2014 et mondialement, il se sera pris dans l'année environ mille milliards (un trillion) de photographies numériques.

Chaque jour, on compte 4,5 milliards de recherches sur Google, 552 millions de connexions à Facebook et 4 milliards de vidéos vues sur You

Tube, site sur lequel 104 000 heures de vidéo sont mises en ligne chaque jour.

En 2012 et 2013, 40 trillions de messages sont envoyés par an, soit 145 milliards par jour (70 % de ces e-mails étant d'ailleurs des Spam*). Fin 2012, on comptait 9 milliards d'objets connectés dans le monde et il y en aura 40 à 80 milliards fin 2020.

Dans le secteur de la téléphonie mobile, on compte 2,3 milliards d'abonnements fin 2013, dont 55 % dans des pays en développement, soit 32 % de la population humaine, 4 fois plus qu'en 2009. Avec ou sans abonnements, le nombre des possesseurs d'un téléphone portable est passé de 750 millions en 2000, à 5 milliards environ en 2013, pour un marché mondial annuel (acquisitions, abonnements, renouvellements, etc.) d'environ 340 milliards de dollars.

L'économie en ligne, elle, représente, en 2013, 2 000 à 3 000 milliards de dollars. En France, « l'e-commerce ne connaît pas la crise ». Au premier trimestre de 2014, il a crû de 11 % selon sa fédération professionnelle. Les plateformes et sites de vente ont augmenté de 17 % en nombre, et 69 % des Français (34 millions de personnes) sont désormais des cyberacheteurs.

Exposée aux actions criminelles, cette galaxie constitue d'autant plus un champ d'action pour les malfaiteurs que l'explosion du volume des données nécessite de les traiter au plus vite, instantanément si possible, ce qui obère les processus de sécurité qui exigent des contrôles et des vérifications, c'est-à-dire du temps.

En matière de cybercriminalité, la prudence s'impose quand on considère les chiffres : on verra en détail que l'état des connaissances en la matière est parcellaire. Le Pr Ross Anderson, qui dirige le Cambridge University Computer Laboratory de l'Université éponyme, doute ainsi fortement des chiffres affolants que trompettent les rapports réalisés ou parrainés par les fabriquants de logiciels de protection. En 2011, par exemple, ils annonçaient que, cette année-là, le cybercrime coûterait 27 milliards de livres au Royaume-Uni. Ce chiffre fit sursauter le Pr Anderson qui réalisa une enquête approfondie dont les résultats nuancèrent fortement les annonces médiatiques sur ce montant. Pour son laboratoire, en effet, quand le cybercrime coûte une livre sterling aux citoyens, la lutte contre lui en coûte dix et, à présent, vaut surtout par son aspect anticipatif. Globalement, le cybercrime causerait un préjudice estimé entre 375 et 575 milliards de dollars, avec un point moyen à 445 milliards

par an. 160 milliards de dollars environ proviennent du vol de données personnelles à des centaines de millions de particuliers. Parmi les pays qui communiquent sur ce point des éléments fiables, on peut citer :

| | |
|---|---|
| Turquie : | + de 54 millions de vols de données (connus), |
| États-Unis : | + de 40 millions, |
| Corée du Sud : | + de 20 millions, |
| République populaire de Chine : | + de 20 millions, |
| Allemagne : | + de 16 millions, |

En outre, le cybercrime provoque la destruction d'un grand nombre d'emplois : environ 200 000 par an aux États-Unis, 150 000 dans l'Union européenne et au total, 500 000 dans le monde. Comment ? Par le pillage de dossiers industriels et de procédés de fabrication, les pirates permettent à des pays sans scrupule de produire et de vendre, en économisant les frais de recherche et de développement, des objets à bon marché provoquant ainsi des destructions d'emplois dans les pays pillés.

# RISQUES ET PÉRILS CYBERCRIMINELS

Qu'est-ce que le cybercrime ? C'est l'ensemble des infractions impossibles à commettre si Internet n'existait pas. Quelle est la gravité de ce phénomène ? Pour les pessimistes, c'est, au choix « la pire des menaces émergentes », la certitude à terme d'une « cyberguerre mondiale » ou « le plus grand transfert de richesses de l'histoire humaine ». Le FBI affirme que, « à l'horizon, le cybercrime émerge rapidement comme la nouvelle menace qui, en matière de sécurité nationale, pourrait bien surpasser le terrorisme ». Pour les optimistes en revanche, le cybercrime est « une broutille dans le cours du business » ou encore « un fétu, comparé à un Produit brut mondial de 70 000 milliards de dollars par an ». Au-delà de ces considérations provenant parfois du terrain, ou à l'inverse, vues de Sirius, un constat s'impose : le cybermonde est d'ores et déjà un nouveau Far West pour une multitude de malfaiteurs et de pirates. Le piratage de la chaîne de grande distribution américaine Target, qui aurait compromis les données personnelles de 70 millions de clients, en est le meilleur exemple.

La criminologie dispose de deux certitudes empiriques : primo, lorsqu'un domaine illicite s'accroît sans cesse et attire toute sorte de

malfaiteurs, c'est qu'ils s'y enrichissent sans grands risques ; secundo, lorsque les particuliers, les États et les entreprises dépensent tous les ans dans le monde et en temps de crise, 48 à 60 milliards de dollars (selon les sources) en sécurité informatique, c'est que la menace est grave.

# Un cyber-jungle ?

La jungle numérique a pour caractéristique première d'être noyée dans le brouillard. Tout y est flou : par exemple, les pertes qu'on prétend y subir vont de quelques milliards à quelques centaines de milliards de dollars. La raison de ce flou tient à ce que, lorsqu'elles le peuvent, les entreprises-victimes cachent ces piratages, et les pertes qu'ils entraînent. Ces piratages prennent de multiples formes qui provoquent une grande variété de préjudices aux sociétés industrielles, financières ou de services qui les subissent. Les vols de propriété intellectuelle sont les plus fréquents et portent au choix ou simultanément sur le résultat de recherches d'une entreprise, ses innovations, ses secrets d'affaires, ses méthodes de fabrication, ses stratégies commerciales, ses contenus d'appels d'offres ou de négociations.

Ces sociétés peuvent également subir des manipulations hostiles de marchés ou de cours de bourse, voir leurs sites sabotés ou paralysés du fait d'attaques en déni de service DDoS, provoquant autant de pertes d'opportunités. Enfin, la confiance qu'elles inspirent ou leur réputation courent le risque d'être malmenées ou détruites par des piratages hostiles. Des particuliers ou des sociétés peuvent également ignorer qu'ils ont été pillés ou être dans l'incapacité d'estimer ce qu'on leur a dérobé en raison de la difficulté de calculer le coût réel de la propriété intellectuelle.

Un dernier risque, enfin, du côté des sociétés de protection informatique : s'informer sur des vols de ce type en procédant à des sondages dans des entreprises, ou en leur adressant des questionnaires peut, volontairement ou pas, fournir des résultats imprécis ou trompeurs.

Quel niveau peuvent atteindre ces pillages ? Nous n'avons sur ce point aucune certitude mais, parfois, une étude spécifique permet de le deviner. Début 2014, une enquête sur le site Pastebin en a donné une idée. Ce site est spécialisé dans le stockage de textes en ligne. Il est normalement utilisé par des informaticiens pour y déposer ou échanger du code et des logiciels mais aussi par des pirates qui y stockent les données confidentielles qu'ils ont

dérobées. L'étude montre qu'en un an, 312 000 identifiants et mots de passe, concernant des sites, des services en ligne ou des gestionnaires de courriels ont été déposés sur Pastebin. Exemple le plus récent : la base entière des données clientèle d'un site pornographique en ligne, destinée à être vendue à des concurrents. Comme les pirates ne déposent pas l'intégralité de leurs pillages électroniques sur Pastebin qui n'est par ailleurs pas unique dans son genre, on peut estimer que, mondialement, les comptes d'utilisateurs piratés se comptent par dizaines de millions.

## Propagande et calculs fantaisistes : les coûts du cybercrime

Le plus souvent, les chiffres disponibles sur les dégâts et le coût de la cybercriminalité proviennent des services de communication des grandes entreprises de sécurité informatique dont on imagine qu'elles n'ont pas intérêt à minimiser la menace. En outre, ces entreprises, pour la plupart américaines, ne disposent de données sérieuses que sur les États-Unis et quelques autres pays, le plus souvent anglo-saxons. En 2013, le cybercrime aurait ainsi coûté 120 milliards de dollars à la seule économie américaine.

Le calcul des profits générés par le cybercrime est tout aussi malaisé. Lors d'un braquage, un bijoutier perd non seulement le prix d'achat de la pièce volée mais également sa marge sur son prix de vente, alors que le braqueur la cédera pour peut-être 10 % de sa « valeur d'échange » à un receleur. Il en va de même pour le milieu criminel du cybermonde dont les profits sont estimés à 104 milliards de dollars par an. La Banque mondiale estime que, pour les années 2012-2013, le coût global du cybercrime est évalué à 300 milliards de dollars par an, soit 0,4 % du Produit brut mondial annuel.

## Quels prédateurs ?

Ils ne sont pas plus bavards que leurs victimes, majoritairement les entreprises. Il est cependant manifeste que l'économie souterraine constitue un important écosystème, une sorte de « cour des miracles » high-tech dans laquelle on trouve tout *via* des sites criminels sophistiqués, parfois analogues aux grandes plateformes marchandes de l'économie licite comme eBay.

Dans cet espace du numérique illicite, s'achète, se vend, s'échange ou se conçoit tout ce qui est lucratif : cartes de paiement, données piratées sur la sécurité, propriété intellectuelle, secrets financiers. Que l'essentiel de ces affaires soit franchement criminel, et non le fait de geeks astucieux, est confirmé par l'UNICRI (United Nations Interregional Crime and Justice Research Institute), organisme spécialisé de l'ONU. Lors de la Global Conference on Counterfeiting and Piracy d'avril 2013, UNICRI a souligné, preuves à l'appui, la proximité entre le piratage informatique et la criminalité organisée transnationale. Ces dernières années, le cyber-banditisme s'est d'ailleurs diversifié et emploie toute une gamme de métiers : codeurs/encrypteurs, diffuseurs de courriels spammés, loueurs de botnets * pour phishing* ou attaques DDoS, hébergeurs de sites illicites sur le Dark web*, etc.

Dans le concret, ce business multiforme et mondialisé fonctionne de la façon suivante : par exemple, des pirates chinois spécialisés dans le siphonage de cartes de paiement embauchent un informaticien russe, ancien du KGB désormais établi au Maroc, pour écrire un code spécifique. Ensuite, cet informaticien monte l'attaque commanditée par ses « collègues » chinois, avec l'aide d'un complice turc qui contrôle un botnet, etc. Interpol estime que, d'ici 2020, le milieu cybercriminel comptera environ un million supplémentaire de pirates de ce type.

# Un cauchemar, et son avant-goût

Aujourd'hui l'ampleur des pertes provoquées par le cybercrime reste supportable. Mais à regarder devant nous et à considérer le développement de la cybercriminalité sous toutes ses formes comme la face cachée du cybermonde, le tableau s'assombrit beaucoup. D'abord, en raison des risques provenant des géants du net eux-mêmes. Ils peuvent être physiques : l'omniprésence du Big Data implique la multiplication des Big Data Centers mais qu'adviendra-t-il si l'une de ces immenses bases est sabotée ou frappée par un attentat ? Peut-on écarter tout risque d'effondrement des réseaux du service public, provoquant anarchie, émeutes et pillages comme à l'a vu lors de pannes géantes ? Quid d'un « écran noir » du Big Data ? Il y a aussi les risques induits par la mégalomanie des mêmes géants du net. On se souvient du début de la guerre en Irak lorsque le Pentagone aspirait à « une vision

divine du champ de bataille » (*God's view of the Battlefield*) : on voit où en est rendu l'Irak onze ans plus tard…

Quel danger représente pour un gigaserveur l'activité d'un « technicien dévoyé » décidé à saboter ou à détruire le système ? La question mérite d'être étudiée alors qu'abondent les preuves de la fragilité préoccupante des grandes architectures informatiques, architectures le plus souvent stratégiques, mais sur la nature desquelles l'opinion ignore à peu près tout. En août 2013, la presse parle d'« une panne informatique sur le Nasdaq qui révèle la vulnérabilité des Bourses », d'une « série noire de dérapages informatiques dans les Bourses mondiales »… La panne de trois heures du Nasdaq fut un choc pour les 3 000 entreprises qu'il cote, notamment Google, Apple et Microsoft. On peut donc légitimement se demander quelle est vraiment la capacité de résistance aux attaques et aux sabotages de cet automate qu'est le Nasdaq. Fin janvier 2014 encore : « La panne de Gmail (le service de courriels de Google) frappe des millions d'usagers au Royaume-Uni, aux États-Unis, en Inde ». 420 millions de particuliers, d'entreprises, etc., éprouvent alors un début de panique.

De fait, le risque de sabotage est clairement identifié pour les méga-superstructures informatiques : des anarchistes et des extrémistes de la « *deep ecology »* travaillent quasi ouvertement à de telles attaques, soit pour « frapper la grande finance », soit pour « sauver la planète ». Parmi les plus fréquemment évoqués, on peut citer des coupures d'électricité massives, des avions cloués au sol, des banques et stations d'essence fermées, l'écran noir de la télévision, l'arrêt de la distribution en grandes surfaces des produits de première nécessité.

Au niveau cybercriminel, les signes inquiétants ne manquent pas non plus. Dans ce pays très attentif à cette nouvelle forme de criminalité qu'est la Grande-Bretagne, le National Fraud Intelligence Bureau annonce que, désormais, 7 escroqueries sur 10 se commettent tout ou partie grâce à l'informatique. On en dénombrait 4 sur 10 en 2009. En 2013, ces cyberfraudes augmentent en volume et en complexité, et auraient coûté 27 milliards de livres à la société britannique. À l'échelle mondiale, les spécialistes de la sécurité informatique signalent une double tendance à l'aggravation et à la spécialisation : désormais, les logiciels pirates les plus perfectionnés proviennent de Russie, les vols les plus audacieux de propriété intellectuelle émanent de Chine, les plus subtiles attaques d'institutions financières, des États-Unis et du Vietnam.

En forte augmentation aussi, les vols de « paquets de données » (*data packs*) par des pirates pour les revendre à des malfaiteurs aux fins de fraudes ou d'escroqueries. Ces « packs » comprennent à chaque fois le nom d'utilisateur d'un individu, son mot de passe et ses numéros de cartes de paiement et de compte en banque. Ces « paquets de données » sont habituellement dérobés dans des bases informatiques mal protégées et incapables de s'en apercevoir, refusant ensuite de rendre ces vols publics afin de protéger leur réputation. Ils donnent accès à des comptes bancaires, Intranets d'entreprise, dossiers médicaux et, plus généralement, à une foule de systèmes informatisés. Aujourd'hui, il y aurait 360 millions de data packs en vente dans le monde.

## Cybercrime : le jackpot

Dernière évolution préoccupante : la recherche du « gros gibier » par les pirates informatiques, à savoir les méga-failles (*megabreach*), c'est-à-dire le siphonage en une seule attaque de millions de dossiers personnels ou d'informations sensibles ; exemple, celle de Target, durant laquelle 70 millions de cartes de paiement ont été potentiellement compromises. Pour les cybercriminels, une *megabreach* en vaut 50 petites. 2013 est l'année de la méga-faille : on en a compté 8 cette année-là, pour une seule en 2012.

Plus largement mais encore à l'échelle mondiale, les actes de piratage, pénétrations de systèmes, etc., ont progressé de 62 % entre 2012 et 2013 ; et les attaques ciblées visant des particuliers ou des entreprises, de 91 %.

Au total, et toujours en 2013, environ 552 millions d'identités ont été mondialement compromises ; et les cyberattaques* ont en moyenne duré trois fois plus longtemps qu'en 2012. Qui plus est, elles ont été encore plus ciblées en direction des personnels sensibles des entreprises : cadres et techniciens, secrétaires de P-DG, etc.

# DERNIÈRES NOUVELLES DU CYBERMONDE CRIMINEL

L'informatique de masse a été développée et popularisée en Amérique. Silicon Valley est située en Californie, l'un des 50 États des États-Unis, superpuissance dont la cyberculture envahit la planète ; commençons donc par ce pays.

# Les États-Unis, berceau et foyer du cybercrime

Vers la fin de l'année 2013, Washington semble brutalement réaliser la gravité du péril représenté par le cybercrime. En février 2014, James Comey, le directeur du FBI avertit ainsi la Cyber Security Conference de San Francisco : « Le péril cyber-sécurité est si grave que, pour la seconde année consécutive, il domine désormais la liste des menaces globales du directeur national du renseignement. Ce péril surpasse à la fois le terrorisme, l'espionnage et, même, celui présenté par les armes de destruction massive ».

Aux États-Unis, tous les clignotants sont désormais au rouge, en premier lieu en Californie, justement. En matière de cybercrime, elle est au premier rang en nombre d'ordinateurs piratés et en pertes financières subies par les victimes, à quoi s'ajoutent les 30 à 40 milliards de dollars qui, chaque année, sont blanchis dans l'économie californienne, le plus souvent par le truchement du cybermonde criminel. À l'échelle fédérale, le nombre d'ordinateurs et de bases de données piratés a bondi de 280 %, de 2009 à 2012. Dès mai 2013, la fédération nationale du commerce de détail des États-Unis a ressenti le « grand basculement » du monde criminel physique vers le monde numérique. Dans son 9e rapport sur « le crime organisé et les détaillants », cet organisme professionnel souligne que la revente des biens volés s'effectue désormais plus sur Internet que par le biais des receleurs classiques comme en témoignent ces deux chiffres : en 2012, 49 % des cas constatés par les détaillants contre 61 % en 2013.

Les fraudes identitaires – achats en ligne illicites, retraits dans des distributeurs automatiques, etc., commis avec des données volées sur le web – atteignent aux États-Unis une dimension épidémique. Durant l'année 2012, des intrusions dans des données personnelles informatisées (dossiers de cartes de paiement ou de sécurité sociale, informations bancaires) ont frappé plus de 16 millions de particuliers résidant en Amérique. En 2013, plus précisément, les fraudes identitaires ont fait 11 millions de victimes : à raison de 4 000 dollars en moyenne de préjudice par incident, cette forme de cybercrime a coûté 24,7 milliards de pertes dans l'année.

Dans le domaine de la santé publique, la situation est relativement inquiétante. Relevant majoritairement du secteur privé, les assurances de santé américaines sont en effet soumises par les pirates à un pillage endémique de leurs données. Un pirate commence par s'emparer de

« l'identité médicale » de la cible puis adresse à sa caisse de (fausses) factures correspondant fictivement à de multiples opérations, analyses médicales, prescriptions, soins. L'argent « remboursé » par l'assurance est ensuite siphonné par le pirate.

Plus stratégiquement préoccupant : le pillage toujours plus intense du secteur des affaires. Fin 2013, un rapport d'un syndicat de directeurs de la sécurité d'entreprises annonçait que 22 % des réseaux qu'ils surveillaient avaient été « cambriolés ». Coût pour ces sociétés : en moyenne, un million de dollars à chaque intrusion, et 2 millions pour le secteur financier.

Désormais contraintes de signaler à la SEC (Securities and Exchange Commission) tout problème de cyber-sécurité, les sociétés cotées le font en nombre toujours plus grand. Les chiffres sont éloquents : 519 attaques significatives en 2012, 1 174 en 2013 ; pour les entreprises pétrolières et gazières : 28 en 2012, 62 en 2013 ; pour les banques commerciales : 36 en 2012, 81 en 2013.

Plus sérieusement stratégique encore : la fragilité du réseau électrique américain face aux cyberattaques. En effet, les grandes sociétés privées du secteur de l'énergie coopèrent peu entre elles ; elles hésitent à divulguer à de potentielles concurrentes leurs informations sensibles et les lois en vigueur ne les contraignent pas assez à protéger leurs réseaux informatiques. Or ceux-ci devraient pourtant s'adapter et se protéger en permanence face à des attaquants qui, eux, évoluent, voire mutent, sans arrêt. Malgré tout, et selon un rapport du Bipartisan Policy Center daté de mars 2014, si le réseau haute tension est décemment surveillé, celui de la basse tension l'est plutôt mal, ce qui risque d'encourager d'éventuels cyber-saboteurs.

# Le reste du monde

Pour l'année 2014, les réseaux d'experts constatent que toujours plus de logiciels ou programmes d'apparence anodine, voire sympathique, jeux, musique, etc. sont piégés et cachent en fait un maliciel (*malware**). Pour le dernier trimestre de l'année 2013 et à l'échelle mondiale, le nombre d'ordinateurs infectés par des « chevaux de Troie » a triplé.

Plus généralement, ces experts signalent les cinq pays au monde souffrant des taux les plus élevés de « cyber-infection », dans l'idée qu'il faut s'y montrer plus prudent encore qu'ailleurs (données de juin 2012, en quantité estimée d'ordinateurs infectés) : Corée du Sud, 57 % ; Chine, 52 % ;

Taïwan, 42 %, puis Turquie, Vietnam, Russie, Inde. À l'inverse, les plus sûrs sont la Suisse avec 18 % et la Suède avec 19 % (suivies par la Norvège, le Royaume-Uni, l'Allemagne et les Pays-Bas).

# Le continent européen

Notons tout d'abord une assez grande ignorance de la réalité des dégâts provoqués par la cybercriminalité sur le continent européen, voire de l'Union européenne. Ce flou se traduit par d'extravagantes divergences sur le coût européen du cybercrime : de 16 à 1 000 milliards de dollars par an ! Europol fournit quand même cette précision : le piratage des cartes de paiement rapporterait annuellement au crime organisé 1,5 milliard d'euros.

Faudra-t-il un désastre numérique pour que l'Europe prenne conscience de la gravité du péril ? Un signe avant-coureur devrait l'y encourager : en juillet 2014, la Banque centrale européenne a été piratée sans qu'elle s'en aperçoive. Des pirates lui ont subtilisé une liste d'environ 20 000 personnes avec adresses (courriels ou postales), numéros de téléphone, etc., listes « parfois non cryptées », puis ont exigé une rançon, que la BCE affirme n'avoir pas payée…

# La Grande-Bretagne

Le ministère britannique de l'Intérieur (Home Office) définit ainsi la cybercriminalité : fraude en ligne, espionnage d'État, fraudes financières à partir d'Internet, attaques sur des réseaux d'ordinateurs, utilisation de virus pour voler des données, usage du cyberespace pour commettre les crimes traditionnels (fausse monnaie et faux en écriture, sabotages, trafics de stupéfiants et trafics d'êtres humains). Ce ministère signale par ailleurs un basculement des éléments les plus inventifs du Milieu, de la criminalité physique vers le cybercrime, ainsi que l'activité dans le pays d'environ 300 cyber-gangs, en majorité issus de l'ex-Bloc de l'Est.

Le Royaume-Uni est le pays européen qui communique le plus en détail sur la cybercriminalité et dont les informations et statistiques sur ce sujet sont les plus complètes. À la suite du piratage d'eBay (jusqu'à 233 millions de fiches clients volées), et aux données compromises de 15 millions de ses clients britanniques, le président de la commission des affaires intérieures de la Chambre des communes en est venu à souligner que l'univers

cybernétique « est désormais l'un des principaux domaines de la fraude et du crime ».

*Les fraudes identitaires* – En Grande-Bretagne, le CIFAS (Credit Industry Fraud Avoidance System) centralise tout ce qui touche à la prévention des fraudes. De janvier à mai 2013, environ 60 000 des 96 000 fraudes qui lui ont été signalées relevaient du piratage informatique, à quoi s'ajoutent 46 000 vols d'identité et 13 500 vols de données ou pénétration d'un compte bancaire. Dans tous ces cas, les systèmes informatiques de vérification et de contrôle mis en place par les détenteurs des données (banques, etc.), ont aisément été contournés ou fracturés.

Au total et cette fois-ci par voie d'enquêtes de « victimation », 221 000 Britanniques auraient été victimes d'une fraude en 2013 soit 600 par jour, dont 129 500 d'un vol d'identité avec 90 % pour ces derniers d'un piratage du compte de leur carte bancaire ou de leurs cartes de fidélité.

*Les piratages de cartes de paiement* – Entre 2012 et 2013, le total de tous les paiements effectués par carte a progressé d'environ 6 % dans le pays, soit 500 millions de transactions supplémentaires, d'une année sur l'autre. Les pertes et préjudices financiers provenant de piratages de cartes de paiement ont augmenté de 16 %, passant de 389 millions (492 millions d'euros) à 451 millions de livres (570 millions d'euros).

Parallèlement, les fraudes sur les chèques (la vieille finance, physique) baissaient de 22 %, de 35 millions de livres (44 millions d'euros) de préjudice en 2012, à 28 millions (35 millions d'euros) en 2013, tandis que les fraudes bancaires en ligne (la nouvelle finance, numérique) augmentaient de 3 % en 2013, de 37 millions de livres (47 millions d'euros) en 2012, à 41 millions (52 millions d'euros) en 2013.

*Préjudices pour la population et les entreprises* – En 2013, plus de 9 millions de Britanniques ont eu un compte en ligne piraté ; 8 % de la population a perdu de l'argent du fait du cybercrime, dont 2,3 % plus de 10 000 livres (12 530 euros) Un piratage dont le niveau atteint 27,3 % des Britanniques dans la tranche d'âge des 18-24 ans. En 2013, le cybercrime aurait causé à l'économie britannique un préjudice de 27 milliards de livres (environ 34 milliards d'euros), dont : 1,7 milliard de livres (2,1 milliards d'euros) pour la fraude identitaire et 1,4 milliard (1,8 milliard d'euros) pour la fraude en ligne.

Pour le « Information Security Breaches Survey » du ministère britannique de l'Économie, 93 % des grandes entreprises du pays et 87 %

des PME avaient subi une cyberattaque en 2012. Des attaques de tous types venant de concurrents, d'hacktivistes, de pirates, de malfaiteurs, etc., qui ont coûté en moyenne 450 000 (565 000 euros) à 850 000 de livres (1 million d'euros) aux entreprises, avec quelques pointes à plus d'1 million de livres (1,25 millions d'euros).

En 2011, 41 % des PME signalaient au minimum une tentative de pénétration de leur réseau informatique par un attaquant extérieur. En 2012, ce chiffre passe brutalement à 61 %. En février 2014, le ministère du Business publie *Crime against businesses – headline findings from the 2013 commercial victimisation survey* qui révèle que, pour les années 2012 et 2013 combinées, les entreprises ont signalé 356 000 cas d'attaques ou de fraudes numériques, pour 85 % d'entre eux des infections par maliciels. En voici le détail (incidents pour 1 000 activités commerciales) :

| | |
|---|---|
| – Maliciels : | 451 |
| – Piratage : | 40 |
| – Sites vandalisés : | 15 |
| – Phishing : | 14 |
| – Vols d'argent en ligne : | 8 |
| – Vols de données en ligne : | 4 |

# La France

À chaque menace nouvelle sur la France, quelle qu'elle soit, l'immuable réaction de sa haute administration s'opère en trois temps : « Ce problème ? Pas chez nous. Ce sont des exagérations journalistiques ! » Seconde étape (quand un drame s'est produit) : « On le savait depuis longtemps ». Dernier temps : « Le problème – réel quoique mineur – est en passe d'être résolu ». S'agissant, à l'été 2014, des risques et périls cybercriminels encourus par la France, nous en sommes clairement au second temps. En avril, une étude portant sur 40 000 cyberattaques (*cf. Le Parisien* du 30 avril 2014) nous apprend que la France est l'un des pays les plus visés. Avec l'Allemagne, la Grande-Bretagne et la Suisse, elle forme un quatuor européen regroupant 71 % des attaques APT (Advanced Persistent Threats)*, présentées comme les plus graves. Les secteurs les plus visés sont les gouvernements et administrations, les domaines de la finance, de la santé et les industries pharmaceutiques, enfin, les télécommunications et les NTIC (Nouvelles Technologies de l'Information et de la Communication).

Depuis 2010, les cyberattaques signalées à la police augmentent en effet fortement, doublant même de cette année-là (626 affaires) à 2012 (1 427). Elles s'effectuent sur tous les supports (ordinateurs, tablettes, smartphones) et dans tous les domaines criminels : prosélytisme, racket, vols d'informations sensibles, vols bancaires, fraudes identitaires, sabotages industriels, destructions de systèmes, surveillance personnelle, etc. Deux domaines semblent spécialement inquiéter les autorités et les professionnels, les escroqueries à la carte bancaire et les siphonages massifs de données dans de grandes entreprises :

*Cartes de paiement* – En 2011, 649 000 opérations frauduleuses sont enregistrées, à partir des plaintes ou déclarations (+ 30 % sur 2010), pour un préjudice total de 413,2 millions d'euros. Les fraudes les plus fréquentes sont les suivantes :

| | |
|---|---|
| – Achat sur Internet : | 52 % |
| – Achat dans le commerce traditionnel : | 13 % |
| – Retraits dans des DAB : | 13 % |
| – Virements bancaires : | 7 % |
| – Autres : | 15 % |

Pour les escroqueries commises sur Internet, le préjudice se monte à 104,2 millions d'euros en 2011, à 109,4 millions d'euros en 2012 et à 125 millions d'euros en 2013. Plus largement, une « étude de victimisation » conduite cette année-là par l'Observatoire national de la délinquance, montre que 2,5 % des ménages ont été victimes de débits bancaires frauduleux. En 2012, la France compte 718 000 victimes, soit 11 % de plus par rapport à 2011 et 43 % de plus depuis 2010. Le débit frauduleux moyen est d'environ 630 euros, pour un préjudice national annuel de quelque 451 millions d'euros, 40 % de ces vols étant perpétrés depuis l'étranger.

*Entreprises* – Début 2014, on apprend que les données personnelles de 800 000 clients d'Orange ont été piratées (3 % du total de ses clients), vol qui ne comprendrait pas les mots de passe des comptes victimes. Seconde attaque à la mi-avril : cette fois-ci, elle concerne les noms, prénoms et courriels de 1,3 million de clients et parfois, leurs numéros de téléphone fixe ou mobile et leur date de naissance.

Un expert commente alors : « En fait, ça arrive tout le temps… Beaucoup d'entreprises sont victimes de ce type de mésaventures ». Pour l'année 2013, les achats en France de logiciels de sécurité (dont les plus sophistiqués sont acquis par des entreprises) se sont élevés à environ

470 millions d'euros. En juillet 2014 enfin, il y a une première alerte aux cryptomonnaies illicites en France, avec le démantèlement d'une plateforme d'échange de bitcoins en ligne qui opérait sans autorisation. 388 bitcoins (soit environ 170 000 euros) sont saisis. Le ministère des Finances lance cet avertissement : « L'activité d'intermédiation consistant à recevoir des fonds de l'acheteur de bitcoins et à les transférer au vendeur de cette monnaie, revient à fournir un service de paiement, activité réservée à un établissement de crédit, de paiement ou de négoce de monnaies électroniques ; toutes activités nécessitant un agrément officiel ».

Il faut noter aussi les attaques DDoS qui, en 2013, ont augmenté de 30 %, selon une société de sécurité informatique sur la base d'un sondage effectué chez ses clients. Avec des victimes notoires comme Orange, Spotify, etc.

# L'Allemagne

En 2013, l'Allemagne a recensé 64 500 cas de piratages (+ 0,7 sur 2012), avec un taux d'élucidation des infractions de 25 %. À l'été 2013, elle a aussi connu une attaque de grande ampleur sur la société de télécommunications Vodafone : vols des noms, adresses, date et lieu de naissance, numéro de compte bancaire de deux millions de victimes. Des complicités internes : un « technicien dévoyé » avait permis aux pirates d'accéder aisément aux informations qu'ils recherchaient.

En janvier 2014, on apprend que 16 millions de boîtes mail ont été piratées, avec leurs mots de passe associés. Des pirates ont « fracturé » les ordinateurs cibles en y installant des « Keyloggers »* (logiciels espionnant le clavier d'un ordinateur) et d'autres logiciels espions « lisant » les champs actifs lors des inscriptions en ligne. Cette opération a permis aux malfaiteurs d'accéder aux comptes de leurs victimes sur les réseaux sociaux et les sites de ventes en ligne. Un butin ensuite vendu au marché noir, sur le Dark web et aux prix suivants : coordonnées de cartes de crédit : un dollar le dossier ; adresses courriel pour du Spam : un dollar les 1 000 adresses.

Enfin, l'Allemagne semble mal contrôler ses sites de paris en ligne et autres « casinos virtuels » grâce auxquels les mafias italiennes, notamment, blanchiraient chaque année des milliards d'euros outre-Rhin.

# L'Irlande

Chaque année, la cybercriminalité coûte à l'économie irlandaise environ 630 millions d'euros, notamment en frais de sécurisation de ses systèmes informatiques, de ses sociétés de gestion de cartes de paiement, etc. 55 % des piratages émanent de cyber-gangs étrangers, installés dans des pays dépourvus de législations réprimant sérieusement le cybercrime et agissant à distance. En 2012, les notifications à la police de piratages ou d'intrusions ont bondi de 32 %. Dans la plupart des cas, les infractions signalées ont été des fraudes identitaires, des escroqueries en ligne, des cyber-pillages ou du cyber-racket.

# Russie et ex-URSS

À travers maints exemples concrets, le lecteur découvrira plus bas l'exubérance de la scène cybercriminelle russe. Soulignons ici simplement que la Russie compte sur son sol, ou dans l'environnement immédiat de l'ex-Union soviétique, 20 ou 30 gangs cybercriminels de taille industrielle. Ils disposent de capacités informatiques analogues à celles d'un État-nation développé et peuvent submerger n'importe quelle cyber-défense, ou pénétrer la plupart des « armures numériques ». Des enquêtes récentes (« Qui sera l'œil de Moscou sur le réseau anonyme TOR », *cf*. références) estiment que le réseau anonyme TOR aurait environ 200 000 utilisateurs en Russie au printemps 2014 (80 000 début 2013).

# Dubaï

En 2014, Dubaï a révélé le niveau atteint dans l'Émirat pour ce qu'on y appelle des « electronic crimes » avec 1 419 cas en 2013 contre 588 en 2011.

# En Chine

Le continent asiatique est une scène très importante pour le cybercrime, en raison du nombre gigantesque des abonnés à Internet, de l'importance et de l'intensité du commerce en ligne, mais aussi jusqu'à présent, d'une sorte d'indifférence, ou de fatalisme des États (hors de la Chine, plus que précautionneuse) face aux activités cybercriminelles.

En 2012, le cybercrime aurait coûté à la Chine la somme de 46,4 milliards de dollars, et l'ensemble des formes de criminalité numérique ferait environ 700 000 victimes par jour dans le pays. Le milieu cybercriminel chinois est très développé : il dispose de son Dark web (marchés clandestins, forums illicites) permettant d'acheter en ligne de multiples outils et services criminels, avec comme cible de prédilection, les 500 millions de possesseurs de téléphones mobiles, dont 81 % se connectent régulièrement à Internet.

Le Dark web chinois propose aussi des « clientèles factices » permettant de faussement placer des applications ou sites en tête des faveurs du public, ce qui leur permet d'obtenir de fructueux contrats publicitaires. La situation n'est pas meilleure à Hong Kong, où les « crimes technologiques » ont bondi de + 36,7 % en 2013, provoquant un préjudice de 44 millions de HK dollars.

# En Malaisie

Ce pays devient l'épicentre de la criminalité nigériane en ligne. Ayant ouvert leur pays aux jeunes étrangers désireux d'y effectuer leurs études, les autorités malaisiennes ont ainsi introduit le loup dans la bergerie : plus de 9 000 « étudiants » nigérians se sont rués dans le pays, souvent, pour y pratiquer la version numérique des fameuses escroqueries à la nigériane.

En règle générale, il s'agit d'un racket aux sentiments ciblant des femmes mûres, solitaires et naïves, surtout des Américaines, « séduites » sur des sites de rencontres. Les pirates nigérians leur content de pathétiques histoires, leur promettent monts et merveilles, en échange de leur aide, puis disparaissent avec leurs économies. En 2013, deux de ces victimes y ont laissé ainsi plus de 250 000 dollars. L'ambassade des États-Unis à Kuala Lumpur a connaissance d'environ 600 de ces cas, les victimes, honteuses ou affligées, étant loin de toutes porter plainte. De tels chantages aux sentiments remportent annuellement plusieurs millions de dollars aux pirates nigérians.

# En Corée du Sud

La Corée recense plus de 100 millions de comptes piratés au début 2014. Or chaque Coréen possède plusieurs cartes bancaires et peut virtuellement vivre sans liquide. En janvier 2014, il est révélé qu'un technicien de 39 ans nommé Park travaillant « à améliorer la protection des clients chez des

émetteurs de cartes », a copié sur un disque portable les bases de données d'un sous-traitant de trois sociétés de cartes de crédit, soit au total les coordonnées non cryptées de 105,8 millions de cartes de paiement. Puis il les a vendues aux concurrents de ces trois sociétés.

## Au Vietnam

Dans ce pays, qui serait « un marché lucratif pour les cybercriminels », le Microsoft Security Intelligence Report révèle en mai 2014 qu'environ 49 % des ordinateurs seraient infectés par des maliciels ou des logiciels pirates. Par ailleurs, 1 % des sites du pays « dissémine des logiciels pirates ».

## En Inde

La cyberfraude (cyber-rançons, vols d'identité, phishing, etc.) a coûté au pays 4 milliards de dollars en 2013. Et 63 % des utilisateurs de smartphones ont, la même année, été victimes d'une forme ou autre de cybercriminalité.

## Mexique

Selon l'Organisation des États Américains (OAS), le cybercrime a provoqué, pour l'année 2013 et à l'échelle du continent sud-américain, un préjudice de 93 milliards de dollars. Et c'est au Mexique qu'il a explosé avec 3 milliards de préjudices en 2013. La spécialité des pirates locaux est le cyber-kidnapping crapuleux : dans un pays où la sécurité informatique est balbutiante, des pirates verrouillent à distance, à l'aide d'un maliciel, le système d'un ordinateur, ou ses bases documentaires, et ne le « libèrent » que contre une rançon de 2 000 à 3 000 dollars, virée sur des comptes à l'étranger.

## Brésil

En 2014, le Brésil compte 107 millions d'usagers d'Internet, soit plus de la moitié de la population. Au total, les cyberfraudes ont causé, en 2012, un préjudice de 1,4 milliard de dollars dans ce pays, dont (selon la Fédération brésilienne des banques) 700 millions de dollars pour les établissements financiers : 95 % des sommes perdues à cause des fraudes relèvent de

l'escroquerie numérique. S'agissant des seules fraudes identitaires, le Brésil est le 10e pays le plus touché au monde et le 2e de l'Amérique latine, avec un préjudice que la banque centrale du pays estime à 86 millions de dollars en 2013.

Le très populaire dispositif de virements en ligne « Boleto bancario », implanté dans les banques, les bureaux de poste, les supermarchés, etc., est utilisé par les gens modestes, dépourvus de comptes en banque, pour payer leurs factures de téléphone, d'électricité, leurs assurances et frais scolaires, etc. Selon la Banque centrale du Brésil, 6 milliards de transactions ont été effectuées en 2013 sur le « Boleto bancario ». En juillet 2014, ce système subit ce qui constitue, pour l'instant, peut-être, le pire pillage de toute l'histoire du cybercrime. Infiltrés dans le système grâce à un maliciel sophistiqué, des pirates ont réussi à y détourner une masse énorme de virements vers des comptes placés sous leur contrôle. 3,75 milliards de dollars ont ainsi disparu, mais les précisions manquent, sachant que 495 793 transactions ont été compromises, avec potentiellement 192 227 victimes.

## En Colombie

L'usage de l'Internet explose en Colombie : 2 millions d'internautes début 2012, 9 millions à la fin 2013. Mais le pays connaît un problème majeur, la fraude identitaire : 43 % de l'ensemble des cas identifiés pour l'Amérique latine ont affecté ce pays en 2013, pour un préjudice total d'environ 95 millions de dollars. En Colombie, 17 % des cybercrimes seraient commis par des pirates, et 61 % par des employés des entreprises, acteurs ou complices. Selon l'Organisation des États Américains, 252 cybercriminels ont été interpellés en Colombie en 2011 ; 323, en 2012 ; 422, en 2013.

# MENACES NUMÉRIQUES POUR LE CITOYEN

Selon le Rapport Norton 2013, le cybercrime coûte mondialement et annuellement 38 milliards de dollars à 128 millions de victimes privées, soit en moyenne 298 dollars pour chacune. Mais dans l'économie de l'information, les plaies d'argent sont loin d'être les seules, ou les plus graves. Car cette société est fondée sur un pacte implicite : le public tolère

d'être espionné sur Internet et les réseaux sociaux, en échange d'une gratuité généralisée. Ce même public ignore toutefois l'intensité de l'espionnage dont il est l'objet. Comme le souligne Julia Angwin dans son inquiétant *Dragnet nation* (*cf*. références) et au regard de ce que pratique au quotidien Facebook sous l'innocent qualificatif de « social mapping » (cartographie sociale), l'ampleur de ce « flicage » généralisé est sans équivalent dans l'histoire.

Peu réglementés, invisibles et silencieux, inconnus du public, le *data mining* et le *digital marketing* traquent et analysent le comportement en ligne des usagers de l'internet, puis vendent ces données à des gouvernements, à des entreprises, voire à des criminels. Cette surveillance de tous les instants rappelle le fameux Panopticon, dispositif architectural carcéral imaginé à la fin du XVIII$^{e}$ siècle par le juriste et philosophe britannique Jeremy Bentham. Un bâtiment circulaire dans lequel l'intérieur de chaque cellule serait visible depuis un unique point d'observation central… Aujourd'hui, Big Brother est dans Big Data et ce que l'on voit d'alors inouï dans le film d'anticipation *Minority Report* est déjà réalisable dans certaines mégapoles : si un fugitif traqué approche d'un écran publicitaire numérique, sa photo y apparaît immédiatement en 4 × 3 m².

Autre forme de cybercrime menaçant bientôt tout un chacun, dans le cours banal d'une activité quotidienne. Un homme boit un verre à la terrasse d'un café après avoir posé devant lui son trousseau de clés. Si les caméras de surveillance du quartier ont été piratées, l'une d'elle captera la marque et le dessin des clés que l'on pourra retrouver dans la base de données (piratée elle aussi) du serrurier, avec le dossier personnel, l'adresse, etc., du propriétaire. Reproduites sur le champ par une imprimante 3D, les fausses clés permettront de cambrioler le domicile visé. Le pire est qu'il n'y aura même pas eu effraction…

Dans l'économie de l'information, la vie privée n'est plus protégeable dès lors que l'on possède un smartphone ou une tablette. Pour quelques centaines d'euros, tout informaticien peut aujourd'hui concevoir un dispositif espionnant tout flux d'information (Wi-fi) circulant sans avoir été sérieusement codé. Car tout système sans fil « fuit » et livre des informations. Comme chaque réseau Wi-fi auquel on s'est un jour connecté reste dans la mémoire du terminal mobile, à toute nouvelle connexion, un serveur récupère la liste complète de tous les réseaux déjà contactés.

## Créer un dispositif de surveillance personnel ? Un jeu d'enfant

À 27 ans, un étudiant de San Francisco a imaginé le dispositif suivant pour un coût très modeste. Avec dix boîtes étanches en plastique (600 dollars), du matériel informatique basique et son ordinateur comme centrale de contrôle, il a capté tout le flux non codé de son quartier. Chaque smartphone ou tablette possédant un code d'identification qui repère sa localisation et devant constamment se connecter à une base pour y récupérer ses messages, cette base sait quel système ce terminal utilise et à quels sites il s'est récemment connecté. Avec son dispositif qui « voit », « suit » et rend compte, l'étudiant a récupéré aisément des adresses e-mails, des photos, des contacts, etc. Mieux encore, quand son dispositif contrôlait un compte courriels, il a pu y introduire des filtres pour en réorienter certains, voire répondre lui-même aux messages de son choix, puis les effacer avant que la cible ne les lise. On imagine sans peine les possibilités offertes dès lors pour espionner un partenaire ou faire chanter les clients d'un « salon de massage ».

Autre type de piège : lorsque quelqu'un regarde un film pornographique sur son ordinateur, il court le risque de voir s'inscrire sur son écran les trois grosses lettres « FBI » et un avertissement à payer sur le champ une amende de 200 dollars. Faute de quoi, l'ordinateur restera bloqué et de sévères poursuites pourront être engagées. 3 à 5 % des personnes rackettées croient à l'authenticité de cette menace et payent. Du côté de Kiev ou de Manille, un pirate gagne ainsi plusieurs milliers de dollars par jour.

## Les nouvelles intrusions du marketing digital

Les pirates du net ne sont pas les seuls ennemis de la vie privée des personnes : les entreprises de marketing digital pistent les consommateurs chaque jour un peu plus grâce aux cookies mentionnés plus haut. Après avoir suivi de près le mode de consommation en ligne de tout un chacun, le digital marketing veut en savoir plus sur l'usager connecté : quels achats a-t-il effectué ? Où vit-il ? Combien d'enfants a-t-il ? Quel modèle de voiture possède-t-il ? Le site de commerce en ligne collecte ainsi les adresses courriels de ses meilleurs clients puis les transmet à une société de marketing qui les intègre dans une base spécifique. Quand le client ainsi fiché visite un

autre site, informé par ladite société de marketing, il est automatiquement dirigé sur les propositions, ou les prix, les plus chers. On est ici dans une variante numérique de la vente forcée, infraction sanctionnée par le code français.

# MENACES NUMÉRIQUES POUR LES ENTREPRISES

Les pillages importants ont débuté en avril 2011 avec la console de jeux Play Station 3 de Sony dont, a-t-on constaté ultérieurement, une clé de chiffrement était défectueuse, car incomplètement aléatoire. Ce défaut a permis aux pirates d'y siphonner quelque 60 millions de comptes, ce qui a coûté sans doute deux milliards de dollars à Sony. Depuis, la situation s'est aggravée sérieusement pour les entreprises, notamment américaines : en mai 2014 par exemple, le directeur du FBI déclare au Sénat : « Il y a deux types de grandes entreprises aux États-Unis : celles qui ont été piratées par les Chinois, et celles qui ignorent qu'elles ont été piratées par les Chinois ». En 2013, 97 % des sociétés du classement Fortune 500 ont subi de sérieux piratages, et les services officiels américains ont prévenu 3 000 entreprises qu'elles étaient piratées, ce que la plupart n'imaginait même pas. Cette année-là, (tous postes confondus), une entreprise de 1 000 salariés devait dépenser environ 9 millions de dollars par an pour sa cyber-sécurité.

Au cours de la conférence « Cost of Cybercrime », une étude a révélé que les cyberattaques avaient en moyenne fait perdre 11,5 millions de dollars aux principaux groupes américains. Ce montant a augmenté de 26 % entre 2012 et 2013…, les plus graves étant les DDoS, les complicités internes et vols numériques, qui représentent 55 % des coûts annuels du cybercrime. Début 2014, on apprend enfin que, pour une entreprise américaine, le coût d'un piratage (ce qu'elle doit payer et non ce que le piratage lui a fait perdre) est passé en moyenne de 3,1 millions de dollars (2012) à 3,5 millions de dollars (2013).

Au salon CE-BIT de Hanovre consacré au high-tech en mars 2014, on a appris que la fréquence mondiale des cyberattaques (connues) de tous types est mondialement passée d'une toutes les 3 secondes en 2012 à une chaque seconde et demi, en 2013. Selon les experts, les plus grands risques sont le vol de données (66 %) et l'espionnage (37 %). Lors de ce CE-BIT, 73 % des directeurs des services informatiques de groupes mondialisés ont révélé

avoir découvert une faille de sécurité lors de l'année précédente. Dans la même proportion, ces directeurs ont annoncé l'augmentation de leur budget cyber-sécurité pour les années à venir.

Deux inquiétantes informations ont encore assombri l'atmosphère : selon la première, désormais 49 % des utilisateurs de smartphones ou de tablettes en usent simultanément pour le travail et les loisirs. Cette pratique suscite d'énormes risques de piratage pour les entreprises, car ces terminaux sont, à 48 %, dépourvus de toute sécurité : ni mots de passe, ni parois coupe-feu ou copies sécurisées. La seconde nous a appris que le logiciel Open SSL, utilisé sur des millions de serveurs et au moins sur 500 000 sites Internet dans le monde, avait été piraté. Ce qui signifie qu'Open SSL a donné aux pirates la capacité de dérober sans laisser de traces des mots de passe, des données de cartes de paiement ou encore des clés de codage.

# La finance, gravement affectée

En 2013, les cyberattaques visant les services financiers de tous types se sont multipliées. Selon le rapport d'une société de sécurité informatique sous-traitante du gouvernement américain, elles représentent 11 à 15 % de toutes celles signalées, devant celles visant les industries de défense. Les techniques de siphonage ont été améliorées : plutôt que de piller les comptes un par un, elles permettent d'infiltrer désormais le système de contrôle des paiements (*master payment switch*) et, à partir de là, de récupérer toutes les sommes disponibles sur autant de comptes souhaités. Simultanément, l'établissement cible est bombardé d'attaques DDoS pour détourner l'attention de ses techniciens.

À l'été 2013, quelques pirates de Russie et d'Ukraine ont été arrêtés après des cyber-pillages dont le montant a atteint environ 300 millions de dollars. Les victimes étaient le Nasdaq (infiltré de 2008 à 2010 sans qu'il le constate), la chaîne de vêtements JC Penney & co., Jet Blue Airways, Carrefour, la chaîne de magasins de proximité 7-Eleven, Citibank, PNC Bank et des filiales de Visa. Au total, 160 millions de références bancaires ou de cartes de paiement auraient été compromises dans l'affaire.

En 2011, le siphonnage d'un serveur de la Croix-Rouge recevant des dons destinés aux victimes de catastrophes permettait déjà à un gang de collecter les coordonnées des cartes bancaires de donateurs en ligne. Les pirates procédaient ensuite à 1 500 retraits dans les distributeurs de 18 pays

et récupéraient au total 14 millions de dollars. Un pirate albanais de 27 ans est arrêté à Stuttgart en mars 2012, puis extradé vers les États-Unis. Mais il n'est qu'un comparse malchanceux d'un cyber-braquage à l'issue duquel les commanditaires et têtes de réseau sont passées entre les mailles du filet.

Au début de l'année 2013, un cyber-gang local a infiltré plus modestement le système informatique d'une succursale de la banque Barclays. Grâce au système KVM (Keyboard Video Mouse, espionnage des frappes du clavier), il a réussi à vider à distance les comptes des clients et à transférer les sommes sur des comptes de complices pour un montant de 2 millions de dollars.

Devant la multiplication des affaires de ce type, l'Association des usagers des banques françaises (AFUB) a dénoncé récemment la passivité des établissements bancaires. En les alertant sur le problème des faux écrans, pratiquement indécelables, se superposant à ceux de la banque et grâce auxquels des pirates du net se présentent aux titulaires de comptes comme leur conseiller bancaire habituel. Leur objectif est évidemment de leur extorquer des informations sensibles ou de leur faire effectuer, sous le coup d'une émotion quelconque, des virements indus.

Devant des problèmes toujours plus massifs et fréquents, les entreprises de sécurité informatique commencent à réagir. Trop souvent, les services en ligne et les applications de leurs clients sont défaillants et un saut de génération devra forcément s'opérer dans la banque de détail. À défaut de quoi, la multiplication des mésaventures comme celles qu'ont récemment connues les sociétés Experian et eBay finira par durablement inquiéter les internautes.

# Le cas Experian

La société américaine Experian est l'un des principaux data brokers* du monde (fournisseurs de données informatiques), activité consistant à vendre des données personnelles de consommateurs destinées aux actions de marketing de ses clients. Elle a pour filiale Court Ventures, société collectant (légalement) des données officielles auprès des administrations, de la justice, etc. Y être abonné permet aussi d'accéder à US Info Search, base de données concernant environ 200 millions d'Américains et contenant notamment noms, date de naissance, numéro de sécurité sociale, adresses actuelles et anciennes, numéro de téléphone, courriel, etc. Tout ce que les

malfaiteurs opérant depuis le dark web recherchent avidement et qu'ils ont baptisé « Fullz ».

Or, de 2007 à 2013, un jeune pirate vietnamien constitue ses Fullz à l'aide de ses abonnements chez Experian/Court Ventures, société qui lui fournit ce qu'il veut sans contrôle de personnalité ; ce Vietnamien vend ensuite 1,3 million de ces précieux dossiers au minimum, à 1 300 voleurs d'identités, fraudeurs et escrocs. Et réalise au passage un gain de 1,9 million de dollars.

Notons ici qu'à partir de ces 1,3 million de Fullz, c'est probablement 30 millions de dossiers qui ont été compromis par la suite en raison de multiples liens et arborescences entre bases de données, ou à l'intérieur de celles-ci,

# Le cas eBay

Fin mai 2014, nouveau vol du siècle en matière de données personnelles : le site de vente en ligne eBay découvre, avec un retard de trois mois, qu'il s'est fait pirater tout son fichier clients mondial entre février et mars, soit probablement 233 millions de fiches. Sur chacune de ces fiches électroniques : l'adresse courriel des clients, leur adresse physique, leur mot de passe eBay, leurs numéros de téléphone et date de naissance : un véritable trésor.

***

Après avoir dressé le tableau des dimensions sans cesse croissantes du cybercrime, nous allons tenter à présent d'expliquer quel est son mode d'action en démontrant qu'en la matière, il s'agit d'abord d'activités criminelles classiques, le cyber n'étant un outil nouveau offert aux malfaiteurs.

## QUATRIÈME PARTIE

# LA CYBERCRIMINALITÉ EN ACTION

En 1985, le sociologue allemand Ulrich Beck publie *La société du risque*[1], ouvrage prophétique dans lequel il décrit notamment ce que, d'après lui, seront les modes d'organisation de l'entreprise de l'avenir. Cet authentique devancier y pressent même le cybermonde criminel, tel qu'il émergera quinze à vingt ans plus tard, dans la décennie 2000. « Les configurations organisationnelles ainsi créées sont moins pesantes, composées de plus petits éléments qui, selon les moments, peuvent être combinés de façon très différente en fonction des circonstances. Chaque "élément organisationnel" peut alors disposer de ses propres relations avec le monde extérieur et mener sa propre "politique extérieure organisationnelle" de façon spécifique à sa fonction. Les objectifs préétablis peuvent être poursuivis sans qu'il soit forcément besoin de consulter la centrale au préalable… etc. ».

Tel est en effet le monde où nous pénétrons désormais. Fruit d'une double mutation, due à la mondialisation et à la cybernétique, sa configuration est inédite ; mais il n'y règne cependant qu'une criminalité classique – banale, pourrait-on dire.

# LES INVARIANTS DU CYBERMONDE CRIMINEL

Dans les sciences (exactes ou humaines), plus confus ou insaisissable est l'objet observé, et d'autant plus impérieuse est l'obligation de fonder ses recherches et analyses sur un sol dont la stabilité permet seule de comprendre et prévoir à temps. Ces pôles de référence se nomment des invariants, concept que, dans sa remarquable *Introduction au siècle des menaces*, le Pr Jacques Blamont expose ainsi : « Dans un paysage où les lignes de force sont exponentielles avec une constante de temps extraordinairement courte, il convient, pour prévoir les activités qui sont liées à cette évolution et souvent créées par elle, de dégager des invariants, c'est-à-dire des concepts autant que possible indépendants de la conjoncture ».

Or quoi de plus conceptuellement insaisissable que l'évanescent cybercrime ? Car en le voyant concrètement opérer, on constate que les

pirates du net agissent depuis les profondeurs du *deep web*, que leur furtivité est telle qu'ils peuvent en quelques secondes dérober des millions de dollars ou de données confidentielles aux plus puissants, aux mieux protégés des géants du net.

Quels sont donc les invariants criminologiques ?

# Le Dark web

L'internet est constitué de différents « étages ». Tout internaute accède gratuitement au « web de surface » où il peut évoluer aisément grâce aux navigateurs classiques. Mais il ignore souvent que, sous cette surface visible, existe un niveau plus « profond », où se trouvent en foule des sites privés et cryptés, licites et accessibles par habilitation ou abonnement grâce à des codes ou des clés spécifiques. Plus bas encore, on accède aux profondeurs du « web obscur », le Dark web.

Tout comme la Cour des miracles, son lointain ancêtre parisien à laquelle on peut le comparer, et même si, comme on le verra plus loin, telle n'était pas sa destination d'origine, le Dark web est aujourd'hui le royaume de l'illicite : forums de discussion, sites marchands, plateformes d'échanges et de rencontre, tous voués à quelque activité illégale dans une gamme ô combien étendue. Des cybercriminels y achètent ou vendent les données confidentielles de cartes de paiement ou de comptes bancaires volés ; on y prépare des cyber-braquages ; on y teste, raffine ou propose ses logiciels pirates (maliciels). Voici un aperçu des services qui sont proposés :

– Siphonner des informations en ligne : un logiciel pirate y coûtera de 200 à 500 dollars.

– Acheter des numéros de cartes de crédit avec mots de passe : on en trouve de 6 à 100 dollars la pièce.

– Envoyer des Spam : un million d'adresses courriel pour 120 dollars.

– Piloter un réseau d'ordinateurs asservis (Botnets) : environ 200 dollars la journée.

– Une discrète installation chez un hébergeur du Dark web : 10 dollars par mois.

– Multiplier le nombre de ses « amis » factices : 115 dollars pour 100 000 « followers » sur Twitter ; 100 dollars pour 10 000 « Likes » sur Facebook.

Par ailleurs, des États ou des entreprises ne se privent pas de recruter au sein du Dark web des mercenaires pour des missions d'espionnage ou de sabotage, comme le signale *Foreign Policy* en juillet 2013 : « Du fait de sa nature amorphe, le crime organisé dans le cybermonde devient un problème crucial, fort difficile à combattre. De fait, des preuves empiriques démontrent que des "hackers-à-gage" y offrent toujours plus leurs services, à la fois à des gouvernements et à des gangs ».

Cependant, force est de constater que, hormis une nature numérique qui lui confère d'emblée un statut mondialisé et une capacité d'action instantanée, le dark web n'offre rien de neuf. En voici une première preuve. Quiconque dispose d'un abonnement à Internet a maintes fois reçu ces courriels émanant de « veuves de généraux nigérians », ou de « la belle-sœur d'Oussama ben Laden », dames généreuses offrant de transférer une fortune au profit du récipiendaire, moyennant un petit virement destiné à « amorcer la pompe ». Ces escroqueries sont connues sous le vocable de « fraudes 419 », du nom de l'article du Code pénal du Nigeria réprimant ce type d'infractions. Mais si ces arnaques sont connues, sont-elles pour autant d'invention récente ? Non : dès 1898, le *New York Times* publiait un long article pour avertir ses lecteurs de cette même escroquerie (bien sûr pratiquée avec des lettres adressées par la poste), alors connue comme l'arnaque du « prisonnier espagnol ».

# La mode du « dark »

Le « dark » est bien sûr le domaine du sombre, de l'invisible. Or loin d'être récent, cet Internet obscur a, au contraire, une longue histoire. Conçu par et pour le Pentagone voici trois décennies, son ancêtre « Arpanet » comportait déjà des serveurs secrets qui lui étaient rattachés en mode invisible. Apparurent ensuite des réseaux privés d'échanges de fichiers, non répertoriés sur les moteurs de recherche accessibles aux seuls initiés.

C'est enfin devenu l'Internet clandestin, à base de sites cryptés et anonymisés, échappant le plus souvent à toute surveillance publique ou privée. En volume, cet espace gigantesque, accessible en ligne mais non indexé, représente quelque 70 % de la nébuleuse Internet ; le « web de surface », celui où accède au quotidien tout internaute, n'occupe que les 30 % qui restent.

# Blackshades : le couteau suisse du cybercrime

Qu'il soit surnommé Blackshades (« Stores noirs ») se comprend, car le nom technique officiel de ce maliciel-espion à usage des pirates amateurs est bien moins excitant : WORM_SWISYN.SM. Mais quel que soit son nom, il est, à l'été 2014, la dernière invention issue du Dark web. Pour un magistrat américain, Blackshades est en effet « une forme effrayante de cybercrime ayant affecté des centaines de milliers d'internautes de par le monde » ; les experts estiment qu'au total, l'« épidémie Blackshades » aurait ainsi infecté 40 grandes villes des États-Unis.

Se répandant aisément par des clés USB, des comptes de réseaux sociaux, des SMS, etc., ce parfait « cheval de Troie » permet de contrôler un ordinateur à distance, à l'insu de son propriétaire. Grâce à Blackshades, le pirate peut, par exemple, activer la webcam et/ou le micro de l'ordinateur de sa victime, récupérer ses mots de passe ou ses données bancaires, dérober tous ses fichiers personnels. Blackshades peut encore lancer des attaques DDoS, identifier les frappes du clavier, s'infiltrer dans d'autres ordinateurs connectés au premier, bloquer contre rançon l'ordinateur cible, etc. Mieux encore : l'achat de Blackshades ouvre l'accès à un site commercial illicite du Dark web où le pirate peut acquérir en ligne des botnets, des outils de cryptage, etc.

Très professionnel dans sa conception, ce logiciel est d'une grande facilité d'utilisation puisqu'« une simple interface, à base de pointer/cliquer, permet aux pirates de voler des données, de consulter tous les fichiers du système, de saisir des captures d'écran, d'enregistrer des vidéos et d'interagir avec toutes les applications de messagerie instantanée et de réseaux sociaux ». Une des victimes de Blackshades a été miss Teen USA, Cassidy W. Un de ses condisciples âgé de 20 ans, étudiant dans le même établissement, commence par infecter l'ordinateur de la jeune fille et à lui envoyer anonymement des photos d'elle nue, manifestement prises dans sa propre chambre depuis son ordinateur personnel. Puis viennent les menaces : « Tu voulais devenir mannequin, tu finiras dans le porno ». Finalement identifié, le maître chanteur est condamné à dix-huit mois de prison ferme. Grâce à Blackshades, il avait au total infiltré 150 ordinateurs.

Cependant, Blackshades tient plus de l'exercice de style que de la machine à s'enrichir. Même s'il est vendu aux environs de 200 euros dans sa formule « Pack premium » (70 dollars pour la version basique), il ne

rapporte aux pirates qui l'ont conçu, Alex Yucel, 24 ans, dit « Marjinz » ou « Viktor Soltan » et à Michael Hogue, dit « xVisceral », qu'environ 350 000 dollars de septembre 2011 à avril 2014, mois où ils sont interpellés. Une somme peu importante au regard des quinze ans de prison que risquent les deux pirates.

Aisément accessible sur un site dédié – étrangement implanté sur le web de surface et non pas dans le Dark web – Blackshades est conçu comme une entreprise commerciale normale puisqu'elle compte deux directeurs, l'un du marketing et l'autre du service clientèle, et un développeur pour entretenir et améliorer la plateforme. Comme un logiciel vendu dans le commerce, Blackshades est livré clé en main avec des mises à jour régulières et une interface conviviale. Pour aider l'apprenti pirate dans ses débuts, il existe une multitude de forums spécialisés dans Blackshades (pour ordinateurs, tablettes ou smartphones…). Il dispose aussi d'une masse de plus de 4 800 *tutorials* (guides de tutorat dans le domaine informatique) ; ainsi que de vidéos accessibles sur You Tube et autres sites en ligne, pour expliquer au débutant son fonctionnement, son paramétrage, etc.

Au printemps 2014, les experts estimaient que Blackshades avait envahi plus de 700 000 ordinateurs au monde, et qu'environ 6 000 pirates l'avaient acheté. Il était donc temps d'agir, avant que l'infection se généralise. Ce printemps-là, une coordination policière internationale lance une grande rafle anti-Blackshades, 350 perquisitions simultanées sont déclenchées dans 8 pays (Belgique, Canada, Danemark, États-Unis, Finlande, France, Grande-Bretagne, Pays-Bas). Mais *in fine*, 80 inculpations seulement sont maintenues : sur 6 000 acquéreurs minimum de Blackshades, l'opération tient plus de l'écrémage que du démantèlement…

## TOR (The Onion Router), la « Piste Ho-Chi-Minh » du dark web

TOR est, une fois encore, un outil numérique inventé, puis diffusé par le Pentagone. En 1996, l'US Naval Research Laboratory, laboratoire de la marine de guerre américaine, invente le concept de « routage en oignon » (*onion routing*) qui consiste à expédier un message à travers une succession de couches cryptées semblable à de concentriques pelures d'oignon. Disposant de serveurs en Islande, en Lettonie et en Roumanie, TOR cache

toutes les adresses IP et crypte fortement tout ce qui s'échange sur le net à travers lui, et à chacune des couches de l'« oignon ». Aucun nœud du réseau ne connaissant la source, la destination ou le contenu des messages qui le traversent, l'internaute dispose sur TOR d'un anonymat quasi-parfait.

Conçu à l'origine comme un navigateur de la 3e génération sur Internet, ce « projet scientifique » vise d'abord à protéger les communications officielles américaines, plus largement à mettre tout internaute en capacité de déjouer les surveillances, la censure et les interceptions. En 2003, TOR est placé en accès libre. En 2012-2013, il est mondialement téléchargé de 30 à 50 millions de fois l'an et utilisé 800 000 fois par jour (+20 % sur 2012) par environ 1,2 million d'individus, tandis que ses outils de navigation s'améliorent sans cesse. Sur le dark web, les sites cachés accessibles par TOR étaient environ 6 500 fin 2013, en majorité criminels.

Dans cette seconde étape de sa vie, TOR devait être voué aux « bonnes causes » telles que rêvées par un libertarien californien : journalistes désireux d'échanger discrètement avec des sources sensibles ou des lanceurs d'alerte, ONG contraintes de communiquer depuis des dictatures, ou des zones infestées de terroristes, militants traqués par leur gouvernement (la « Révolution verte » en Iran, en 2009 ou le « Printemps arabe », en 2011), entreprises voulant protéger leurs affaires de la concurrence, persécutés ou victimes, recherchant un canal protégé d'échange.

Pour le Congrès américain et le State department, TOR devait être un « facilitateur de la liberté en ligne ». Or comme il était prévisible, il est rapidement devenu un outil de choix pour les cybercriminels. Depuis, le dark web accessible par TOR accueille en foule sites, messageries, forums et plateformes illicites pour des trafics de stupéfiants, d'armes, ou d'êtres humains, du blanchiment d'argent, l'achat ou la vente de logiciels piratés. En 2014, la conjonction de TOR, des bitcoins et du réseau privé VPN* constitue le « cyber-pack » le plus recherché du monde criminel numérique.

La protection qu'offrent ces outils cryptés est-elle pour autant parfaite ? Pas totalement, même si les sites TOR les plus discrets changent leurs adresses plusieurs fois par jour… Nous verrons plus bas que le démantèlement, en octobre 2013, du site Silk Road (sorte d'eBay des stupéfiants) ou, en août 2013, celui de Freedom Hosting, logeant des sites pédopornographiques comme « Lolita City », « Love Zone », ou « Pedo-

Empire », n'auraient pu se réaliser si les gestionnaires et usagers de ces criminelles plateformes étaient restés pleinement anonymes…

C'est pourquoi des cybercriminels russes ont voulu créer leur propre version de TOR. Au printemps 2014, la méga-meute criminelle Zero Access Botnet, qui contrôle 2 millions d'ordinateurs « kidnappés » de par le monde, aurait entrepris de créer son propre réseau peer-to-peer qui lui permettrait de pratiquer tous les échanges, transferts et attaques de son choix dans un authentique anonymat. Surtout, sans que la NSA ou la CIA ne vienne l'espionner.

Du fait de son degré élevé de sophistication et de son caractère de dédale multidimensionnel, le Dark web est, pour l'instant, quasi inexpugnable, et permet à ceux qui s'y dissimulent de gagner des milliards. Parmi les plus inventifs du Dark web, les pirates issus de l'ex-Bloc de l'Est (durant la guerre froide : URSS et ses pays satellites) mènent depuis ses profondeurs des activités criminelles clandestines de grande ampleur : organisation de campagnes de Spam, vente en ligne de faux médicaments, rackets et fraudes identitaires ou autres. Au total, la piraterie russe représenterait un tiers de la cybercriminalité globale pour un chiffre d'affaires de plus de 2 milliards de dollars par an et la moitié environ des sites marchands cybercriminels repérés serait russe.

## UN CYBERCRIME ORGANISÉ AUX PRATIQUES PLUTÔT CLASSIQUES…

Nous avons déjà évoqué diverses cyberattaques, spectaculaires par leur ampleur ou leur sophistication. Pour plus de précision, voici le détail de certaines d'entre elles, parmi les plus dangereuses.

### Braquages cybernétiques

Là aussi, on constate le « grand basculement » entre vols à main armée physiques et ceux pratiqués dans le cybermonde. Dès 2012, le FBI signale ainsi la baisse des braquages physiques de banques : en 2010, il en compte 5 000 alors qu'un an plus tard, ils ne sont que 3 870, soit une baisse de 23 %. Cette tendance se confirme et montre que la criminalité se déplace vers de nouvelles formes de braquages, moins risquées et bien plus

lucratives : quel vol à main armé a-t-il jamais rapporté des dizaines, voire des centaines de millions de dollars ? Comme le rapporte CNN en juillet 2013, « les cyberattaques sont les braquages de l'avenir… Les braqueurs ne portent plus de cagoules et ne brandissent plus d'armes ». Le syndicat professionnel des banquiers américains l'affirme : « La fraude électronique va augmenter ». Pour l'année 2012 et dans le monde entier, les cyber-braquages auraient au total rapporté environ 11 milliards de dollars aux pirates et aux commanditaires qui les exploitent. En 2013, on estime que 740 millions de données personnelles ont été compromises, le pire chiffre depuis que ce genre de statistiques existe. En février de cette année-là, un seul de ces cyber-braquages a rapporté 40 millions de dollars.

Quels sont les facteurs dont profitent les pirates ? Alors que les cartes bancaires européennes sont sécurisées à 95 % par des « puces », à 79 % pour le Canada et tout le reste du continent américain (Amérique centrale, Amérique du Sud, etc.), celles des États-Unis (27 % des cartes mondiales) ne le seront pas avant (peut-être) 2015, en raison de l'hostilité des lobbies des banques et du commerce qui rechignent à prendre en charge le coût de la transition de la carte à piste magnétique vers celle à puce, soit 8 milliards de dollars.

Quelles sont les diverses étapes d'un cyber-braquage réussi ?

Étape 1 – des pirates repèrent, puis infiltrent, le système informatisé d'une société du sous-continent indien, sous-traitante d'un géant mondial de cartes de paiement, et y siphonnent les données de dizaines de milliers de cartes prépayées sans « puces » électroniques, les informations étant encodées sur de simples pistes magnétiques.

Étape 2 – les pirates fabriquent des cartes clonées, comportant les numéros et codes de celles qu'ils ont subtilisées. S'introduisant à nouveau dans les dossiers d'origine de ces cartes, ils en augmentent les plafonds de débit (celui qui empêche, par exemple, de retirer plus de 1 000 euros par semaine dans un distributeur automatique) : si une carte a un plafond de 10 000 dollars, leur seuil d'acceptation est poussé à 100 000 dollars, et ainsi de suite.

Étape 3 – les cartes clonées sont distribuées à des complices (Colombiens, Néerlandais, etc.) qui, en quelques jours, vident des dizaines de milliers de distributeurs de billets dans différents pays : dans la seule ville de New York, 2 904 d'entre eux ont été pillés en dix heures pour un butin de 2,4 millions de dollars.

Une opération sans risque car, contrairement aux cartes personnelles, les prépayées n'appartiennent à aucun individu particulier : faute de plaintes de victimes remontant vers la société émettrice des cartes, les retraits abusifs passent inaperçus et peuvent durer longtemps.

Ce pillage affecte d'abord le Canada, la Colombie, l'Égypte, les États-Unis, le Japon, la Roumanie, le Royaume-Uni, la Russie, le Sri Lanka où les cyber-braqueurs multiplient retraits et achats de produits de luxe (ensuite revendus).

Autre forme de cyber-braquage, rendue publique en juin 2014 après l'arrestation d'un gang roumain qui proposait à des patrons de bars et restaurants (aux États-Unis, en Russie, au Pakistan, en Serbie, etc.) un maliciel qu'il leur suffisait d'adapter à leurs terminaux de paiement. Ce maliciel captait les données des cartes bancaires utilisées par leurs clients. 6 600 cartes ont ainsi été piratées puis utilisées pour des retraits d'espèces ou des achats en ligne.

Les vols au goutte-à-goutte, consistant à prélever des sommes aussi minimes qu'anodines sur de nombreux comptes – moins de 10 dollars –, se multiplient aussi, en particulier durant les périodes de vacances où l'on achète davantage sans surveiller régulièrement ses comptes.

## Des cyber-gangs opérant comme des entreprises

Entre Dark web, bitcoin et réseaux TOR, de véritables SSI criminelles (sociétés de services informatiques) opèrent désormais. Tout comme celles du monde licite, ces « cybermarchés noirs », ou « services criminels à la demande » disposent de leurs propres réseaux de communications, de leurs services de relations humaines (recrutement de techniciens à vocation de pirate, etc.), de leurs directions du marketing et des contacts avec la clientèle, parfois même d'une aide en ligne pour les clients novices.

Acceptant toutes sortes de cybermonnaies, elles sont rompues aux techniques de la promotion commerciale : une entreprise souhaite-t-elle louer un Botnet pour deux mois afin d'assommer les ordinateurs (ou les tablettes, ou les smartphones…) de son concurrent sous les attaques DDoS ? On lui suggérera de pousser le marché à trois mois, ce qui lui vaudra un quatrième mois d'utilisation gratuit… voire à lui céder à bon prix le code source du Botnet utilisé régulièrement.

Prenons l'exemple de Citadel-Botnets, dont le chef est surnommé « Aquabox » sur Internet. C'est une entreprise illicite qui, après agrément d'un futur affilié, vend pour quelques milliers de dollars un « Kit-Citadel » à qui le sollicite. Grâce à ce logiciel pirate, le nouvel associé pourra créer son réseau d'ordinateurs asservis (Botnet) et le faire fructifier. Notons, au passage, une nouvelle preuve du fonctionnement classique du cybermonde criminel : le mode d'organisation de Citadel est celui, séculaire, d'une « famille » mafieuse sicilienne. Chacun des propriétaires de Botnets travaille à son propre compte mais plusieurs d'entre eux peuvent se regrouper afin de monter de grosses opérations, ou louer leur réseau à un autre affilié. Au total, la « famille » Citadel contrôlait ainsi, jusqu'à l'été 2013, 1 400 de ces Botnets, soit une force de frappe mondiale de 5 millions d'ordinateurs asservis. En 2012-2013 par exemple, Citadel a ciblé le gotha bancaire mondial et quelques géants du net : American Express, Bank of America, Citigroup, Credit Suisse, HSBC, JP Morgan-Chase, Royal Bank of Canada, Wells Fargo et PayPal, pour un butin connu de 500 millions de dollars.

Citadel dispose, en outre, d'une organisation très élaborée puisque l'achat de son « Kit-Citadel » donne au néophyte accès à des forums secrets d'échanges et de coordination, ainsi qu'à des « guides des bonnes pratiques » avec cette indication intéressante : parmi les règles imposées aux affiliés, Citadel stipule l'interdiction de cyber-braconner en Russie ou en Ukraine. Un millier de Botnets/Citadel a été démantelé en juin 2013.

# Cyber-voleurs et pillards de données

En 2009, un groupe de pirates de l'ex-URSS nommé « Cyclosa Gang » a créé SSNDOB, un site de vente d'informations personnelles volées. Pour les récupérer, SSNDOB attaque et pille les bases documentaires de grandes entreprises, de banques ou de caisses d'épargne, sans oublier des vendeurs d'informations personnelles licites, comme Lexis Nexis, Kroll ou Dunn & Bradstreet. Des victimes qui ont parfois mis cinq mois à réaliser le vol de leurs fichiers.

SSNDOB détenait ainsi 4 millions de dossiers de futures victimes, surtout Américaines, informations achetées par quelque 1 300 « clients ». Mais dans la jungle du Dark web, les pirates se dévorent entre eux : à l'été

2013, SSNDOB se fait à son tour siphonner toute sa base de données, probablement par des hacktivistes américains.

## « Zero day* exploits » : un sésame numérique

Au cœur du monde des voleurs d'informations figure le marché des failles exploitables, dites « Zero day exploits », ZDE, c'est-à-dire les défauts dans la cuirasse de sites, réseaux ou serveurs, le plus souvent marchands, ou officiels. C'est le domaine des pirates les plus doués, mais invisibles car enfouis au plus profond du Dark web. Le marché des ZDE explose d'autant plus que des fortunes s'y gagnent au quotidien et en toute impunité, dans un silence de cathédrale et sans que la moindre ride n'agite la surface des eaux. Ces puissants pirates sont en mesure de vendre aussi bien les références de comptes bancaires ou de cartes de paiement que des virus, le contrat de commission d'un cyber-attentat visant le site d'un concurrent que des logiciels pirates, etc.

Leur nec plus ultra est ces « failles exploitables » par défaut ou erreur de codage dont on peut user sur le champ (d'où *zero day exploit*) pour infiltrer un logiciel et en prendre le contrôle. Dans le monde physique, l'équivalent serait un cambrioleur entrant dans la salle forte d'une banque par une porte dérobée dont il posséderait la clé et repartirait avec l'argent sans laisser de traces ni avoir déclenché l'alarme.

Quand un pirate découvre une faille, qu'il s'y infiltre lui-même ou qu'il la vende, il faut en moyenne 300 jours pour que le concepteur du logiciel s'en aperçoive et « referme la porte ». En 2014, une belle « faille exploitable » vaut environ 250 000 dollars. Qui va l'acheter ? Tout le monde, d'un service officiel américain aux Gardiens de la révolution iraniens, auxquels s'ajoute le secteur privé ou des amateurs doués. Dans un Dark web toujours plus professionnel, des intermédiaires, ou « tiers de confiance », ont désormais pignon sur rue. Certains ont des sites, ou des forums, spécialisés pour certains dans les ZDE bas de gamme payables de 10 à 1 000 dollars en bitcoins, comme <1337day.com>, actif à l'été 2014.

Bien connus des « collectionneurs », d'autres intermédiaires, eux plus haut de gamme, vendent des ZDE plus exclusives, moyennant une ristourne de 15 % sur le prix de vente, plus une prime mensuelle payable tant que la « faille » reste ouverte. Aller sur les sites et forums du Dark web spécialisés en ZDE est éclairant : les demandes et propositions y sont parfaitement

explicites. Et souvent inquiétantes : on y « vend » en effet couramment les « failles exploitables » permettant d'accéder aux systèmes de centrales électriques, de stations d'épuration d'eau, de raffineries de pétrole.

## « Heartbleed » : la ZDE-faille-catastrophe

En avril 2014, *Le Monde* titre : « La faille qui frappe le cœur de la sécurité sur Internet ». Et de fait : celle qui porte le nom austère de « CVE-2014-0160 » dans la « base documentaire des vulnérabilités » et dont le nom de code est « Heartbleed », est sans doute le ZDE de la décennie. Dans la barre des adresses de son navigateur Internet, chacun peut voir, à gauche, l'icône du logiciel Open SSL. Après passage au programme https*, ce petit cadenas annonce la mise en sécurité, par chiffrage* des données, des transactions entre le navigateur et le site web consulté.

Or en décembre 2011, une erreur de programmation a fragilisé la nouvelle version du code Open SSL mise en ligne en mars 2012, sans que l'erreur n'ait été détectée ni corrigée. Une porte existe donc dans le système « sécurisé » et elle va rester silencieusement ouverte durant plus de deux ans. Grâce à elle, un pirate bien informé peut accéder, sans laisser de traces, à une foule d'informations personnelles, supposées inaccessibles car cryptées : identifiants et mots de passe, clés de chiffrement, etc. Ce qui fait craindre d'énormes dégâts potentiels pour des réseaux sociaux, des sites bancaires ou de commerce en ligne, voire pour des routeurs comme ceux de Cisco (le numéro un mondial des réseaux informatiques). Refermer la porte et combler la faille décelée n'est pas simple : il faut d'abord corriger le code sur un serveur, puis demander à chaque utilisateur du site concerné de pratiquer une mise à jour système.

Qui a utilisé « Heartbleed » ? Quels dégâts a-t-elle réellement provoqués ? Dans cette affaire, rien n'est encore certain et les enquêtes sont toujours en cours. Reste à espérer qu'elles aboutiront, d'autant plus qu'à l'été 2014, Open SSL Foundation a révélé que de nouvelles vulnérabilités avaient été décelées sur le logiciel éponyme.

## Target : la méga-faille du siècle – ou celle de l'année 2013 ?

Comme partout ailleurs, il y a des modes en matière de piratage numérique : en 2013, la tendance était ainsi au pillage des terminaux informatisés des points de vente (*point of sale attack*). Dans ce cas, ce sont les données récoltées dans le réseau informatique d'un magasin donné qui sont ciblées, pas le site web de la chaîne elle-même, supposé mieux protégé. C'est ainsi qu'en pleine saison des achats en ligne, dans le mois qui précède Noël par exemple, quand le chiffre d'affaires des sociétés spécialisées augmente de 50 %, le géant de la distribution Target, la 3e chaîne des États-Unis, a subi un gigantesque piratage lors duquel les données de 40 millions de cartes de paiement utilisées du 27 novembre au 15 décembre 2013 ont été siphonnées. À partir de là, on considère que les informations personnelles de 70 millions de clients ont été aussi potentiellement compromises. À supposer que tous les possesseurs des cartes piratées chez Target s'y fassent dérober chacun la somme maximum de leur plafond de crédit, le préjudice total serait alors de 4,1 milliards de dollars…

Qui sont les pirates ? Ils sont sans doute originaires de l'ex-URSS, les données Target ainsi subtilisées étant destinées à être vendues sur le Dark web, pour un profit estimé à 50 millions de dollars. Les experts soupçonnent que, au cours des années précédentes, ce gang a déjà pillé les données de millions de cartes bancaires à la chaîne de grands magasins Neiman Marcus, à la banque Citigroup, au détaillant de sportswear JC Penney, etc.

Pour opérer chez Target, ils ont utilisé comme cheval de Troie la société de service du distributeur (nommée HVAC) qui entretient l'air conditionné, le chauffage, etc. Après avoir récupéré ses mots de passe, ils n'ont plus eu qu'à infiltrer le système de Target, puis à le piller sans qu'il s'en aperçoive : l'intrusion a duré quasiment un mois et ce sont les services officiels américains qui ont averti sa direction de la sécurité.

Ce pillage géant de données est loin d'être le premier : on a fini par apprendre que le grand soldeur américain TJ Max et sa filiale anglaise en ont été victimes en 2007. Ce qui n'a pas empêché les géants du commerce de se montrer négligents en matière de protection de leur informatique. La sécurité de Target a d'ailleurs signalé en son temps une activité suspecte dans son système, sans doute un piratage. Mais fallait-il le révéler en plein *boom* d'avant Noël ? La direction de Target a choisi de ne pas donner suite, se bornant, le désastre survenu, à publier un communiqué en pure langue de bois : « Rétrospectivement, nous nous demandons si le fait d'avoir, à

l'époque, porté un autre jugement sur cette affaire n'aurait pas entraîné une issue différente »…

Au trimestre suivant, les profits de Target ont baissé de 46 % : entre les remboursements aux clients, les frais d'avocats et de justice, les vérifications internes et changements de logiciels, l'affaire lui aura coûté 420 millions de dollars auxquels s'ajoute un préjudice d'environ 200 millions pour ses banques. *In fine*, la direction de Target a conclu à la nécessité de se doter d'un directeur de la sécurité informatique…

# Et toujours les DDoS

Pour le commerce en ligne, l'attaque en déni de service DDoS constitue un réel danger. Durant la saison des fêtes de fin d'année, une attaque paralysante sur un important site de commerce en ligne peut, en effet, provoquer une perte directe de 500 000 dollars de l'heure. En y incluant des dommages indirects à la réputation de la marque, l'heure de paralysie peut coûter plusieurs millions de dollars.

De plus, les attaques DDoS sont toujours plus fréquemment utilisées comme arme de diversion car elles permettent de détourner l'attention du service de sécurité informatique d'une cible, pendant que les pirates exploitent par ailleurs une faille dans le système. Pour l'année 2013, selon des experts en sécurité informatique, 40 % des attaques DDoS repérées avaient une origine « politique », idéologique ou liée au fanatisme, 39 % d'entre elles avaient un objectif indiscernable et 16 % constituaient une diversion en vue d'un pillage.

Le *State of Internet Report* du troisième trimestre 2013 apprend ainsi que, sur 127 attaques DDoS visant des entreprises ou administrations américaines, 80 ciblaient le secteur du commerce, 42 ceux des médias et du divertissement, 18 celui de la fonction publique et 14 celui du High-Tech. Un sondage annexé au rapport soulignait que 45 % des administrations ou entreprises interrogées avaient subi une attaque DDoS dans l'année et que 21 % d'entre elles ne possédaient aucune équipe formée pour répondre à de telles attaques.

Plus intéressant encore, les services de surveillance officiels ou privés constatent que 25 % de toutes les attaques DDoS pratiquées au monde proviennent d'Inde, de Chine et d'Iran, le reste des attaques de ce type étant

réparti entre une vingtaine de pays, chacun représentant moins de 3 % du total.

Depuis le premier semestre 2014, les attaques DDoS se sont multipliées à travers le monde et visent désormais les applications ou des objets connectés, comme des caméras CCTV. Un expert estime que ce dernier type d'attaques pourrait augmenter de 240 % dans l'année 2014. Sur les sites spécialisés du Dark web, la location de Botnets pour commettre tous les méfaits possibles est désormais bradée, parfois à moins de 10 euros l'heure…

# Cyber-espions

Le cyber-espionnage consiste à voler sur le web des informations ou données secrètes ou sensibles provenant du monde des affaires ou des administrations, mais aussi les centres de recherches universitaires. Dès le début de la décennie 2010, on a ainsi constaté un net accroissement d'attaques visant ceux des États-Unis avec 90 000 à 100 000 tentatives par jour parfois, pour des centres de recherches de taille moyenne. Sur l'ensemble de ces centres, les intrusions ou tentatives hebdomadaires se comptent par millions.

Les universités ont une importante activité intellectuelle, elles déposent des brevets, inventent des appareils ou logiciels nouveaux, etc. Non seulement leurs réseaux informatiques sont plus ardus à protéger que ceux des entreprises mais il est en outre difficile d'estimer ce qui leur a été dérobé. Ces « effractions » furtives et indirectes proviennent le plus souvent de Chine, de Russie ou du Vietnam. Elles sont difficiles, sinon impossibles à identifier car les pirates usent de multiples ordinateurs et passent par plusieurs pays coupe-circuit.

# Cyber-kidnappings ou enlèvements numériques

Connu sous les noms de « Lucky12345 » et de « Slavik », Evgeniy Mihaïlovich Bogachev, 30 ans, dirige le cybergang « GameOverZeuS », ou GOZeuS*, dont l'« arme numérique » majeure est un logiciel pirate conçu pour « flairer » et traquer les fichiers contenant des informations financières. Ce logiciel cherche les codes d'accès aux comptes bancaires de sa cible et à toutes ses autres informations financières, puis enclenche le

dispositif de « kidnapping » « CryptoLocker ». Celui-ci verrouille toutes les données financières de l'ordinateur de la victime en les codant successivement deux fois, puis lui réclame une rançon en bitcoins. En quelques mois, cette redoutable cyber-arme financière aurait rapporté 27 millions de dollars et plus d'un million d'ordinateurs dans le monde seraient infectés par « GOZeus », dont 25 % aux États-Unis.

L'Amérique latine n'est pas épargnée par ces kidnappings numériques : en Bolivie, par exemple, un cyber-gang traquait voici peu sur les réseaux sociaux et Internet des victimes potentielles de kidnapping physique. Une fois l'individu « radiographié », ce gang l'enlevait et fixait en toute connaissance de cause le montant de la rançon. 17 personnalités ont ainsi été récemment enlevées pour des rançons de 200 000 dollars et plus. Le chef de ce gang hybride était un… pasteur évangélique. La plupart des victimes n'ont pas osé porter plainte. Et la Bolivie n'a toujours pas de lois efficaces contre la cybercriminalité.

En France, une chaîne de livraison de pizzas à domicile a été prise en otage par le cyber-gang Rex Mundi qui, en pleine coupe du monde de football, lui a siphonné les données de 650 000 de ses clients en France et en Belgique. Le gang exigeait une rançon de 30 000 euros en bitcoins que ladite société a prétendu ne pas avoir payée. En 2012, Rex Mundi avait déjà tenté de racketter la société Numéricâble et la banque Dexia, en cryptant leurs bases de données et en proposant de déverrouiller ce cryptage contre rançon. Les deux entreprises ont elles aussi affirmé avoir refusé de payer. Au niveau mondial, ces kidnappings d'un nouveau genre auraient été multipliés par six depuis 2012.

# Trafics de stupéfiants dopés au numérique

Au début de la décennie 2010, des pirates engagés par des cartels latino-américains de la drogue sont parvenus à infiltrer les systèmes informatiques de deux éminentes sociétés maritimes de transport par conteneurs. De 2011 à 2013 (estimation minimale) ces narco-pirates ont espionné le dispositif logistique de localisation des conteneurs destinés au port d'Anvers et appris leur identification, leur contenu et leur localisation précise. Rien de plus aisé, ensuite, que de placer des cargaisons de cocaïne, ou autre drogue, dans certains de ces conteneurs, puis de les récupérer à l'arrivée avant que le destinataire les réceptionne et les fasse inspecter par

les autorités portuaires et douanières. Quand le subterfuge fut découvert, les douaniers mirent la main, en une seule rotation, sur une tonne de cocaïne et une tonne d'héroïne. On imagine la quantité de stupéfiants qui, en deux ans, a été ainsi introduite en Europe.

## Fraudes et blanchiment : les casinos du Dark web

Les casinos en ligne prolifèrent désormais dans le web de surface mais aussi dans le dark web et leur nombre augmentera sans doute encore de 30 % d'ici à 2018. Au point que d'ores et déjà, les casinos en ligne licites, agréés, ne représenteraient plus qu'environ 10 % du total estimé. Très clairement destinés à blanchir les revenus générés par des activités illégales, une grande partie de ces casinos du Dark web s'est rendue anonyme et intouchable en n'utilisant que des monnaies numériques.

## L'industrie nouvelle du chantage sexuel en ligne (« sextortion »)

Le principe consiste à compromettre une personne fragile avec des photos, des enregistrements puis de la faire chanter en la menaçant de tout révéler. Les possibilités offertes par Internet et les réseaux sociaux ont transformé en une véritable industrie ce qui n'était naguère qu'un sordide artisanat.

Qu'on imagine d'immenses bureaux, style centres d'appels, dans lesquels s'agite un personnel ayant reçu une formation spécifique et d'autant plus motivé qu'il reçoit des primes si ses objectifs de chantage sont atteints. Des « séducteurs » des deux sexes draguent ainsi leurs victimes sur Internet, lors de « chats » ou sur des réseaux sociaux, puis les invitent à des cyber-jeux sexuels qui sont intégralement enregistrés. À la fin, le séducteur devenu racketteur menace de tout mettre en ligne, si une rançon (de 500 à 15 000 dollars, selon les cas), n'est pas versée.

Parfois, les victimes sont rackettées à plusieurs reprises. Il a été prouvé que plusieurs suicides d'adolescents, incapables de payer ou d'avouer, ont eu ce chantage pour cause. Ces cyber-racketteurs sont surtout implantés aux Philippines, et ciblent des victimes établies à Singapour et en Indonésie, et

jusqu'aux États-Unis, en Grande-Bretagne et en Australie. En Afrique, des gangs analogues ciblent plutôt des Européens.

# LES PRINCIPAUX MARCHÉS CYBERCRIMINELS

L'observation empirique permet de confirmer la robustesse et le dynamisme de ces marchés criminels numériques car, quand disparaît l'un de leurs acteurs, il est remplacé sur le champ. Et l'on constate aussi qu'une sorte de code de conduite est en vigueur entre les acteurs de premier plan du cybermonde criminel : on ne s'attaque pas, on ne se pille pas les uns les autres. Ce « code » est-il implicite ou explicite ? Aujourd'hui, nulle réponse claire n'existe.

Pour l'essentiel, ce cybercrime organisé agit aujourd'hui à sa guise. Face à lui, l'amateurisme, la désorganisation, le chacun pour soi et plus grave encore, l'irénisme, voire une complicité libertaire.

## La fraude identitaire aux États-Unis

Nous avons déjà évoqué ce type de fraudes à propos du pillage du secteur américain des assurances de santé. Le recueil des données peut s'opérer par piratage informatique mais également en volant des ordinateurs portables ou des tablettes à usage professionnel appartenant à des cadres des sociétés visées et contenant des fichiers intéressants. Ou encore en soudoyant des employés aigris, mal payés ou corrompus, à l'aide de « cadeaux » : souvent des « fêtes » agrémentées de stupéfiants et d'*escort girls*.

Sur le Dark web, les filières de piratage de données personnelles fonctionnent de la façon suivante. Des codeurs inventent un « maliciel » original destiné à récupérer des données identitaires sensibles. Celui-ci est ensuite vendu à des pirates qui l'utilisent pour pénétrer des bases de données et y récupérer de quoi assembler le plus possibles de Fullz. Ces Fullz sont ensuite revendus à des escrocs spécialisés dans des fraudes identitaires, voire à des sociétés légales (mais souvent opaques…) de marketing numérique. Quelques mois plus tard, le maliciel déjà bien

exploité et rentabilisé est vendu d'occasion sur des sites « gris », au bénéfice d'amateurs et de débutants.

Étant donné la multitude de démarches aujourd'hui accomplies en ligne, ces filières permettent des fraudes et escroqueries aux dépens de victimes dont l'identité numérique a été clonée. Selon un sondage par secteur professionnel opéré en 2013 par le Identity Theft Resource Center sur le nombre d'intrusions informatiques visant la fraude identitaire, 267 intrusions, soit 43 % du total, portent sur le monde de la santé, 210, soit 34 % du total, sur celui des affaires et 23, soit 3,7 % du total, sur celui de la finance.

# Le domaine de la santé

En 2013, plus de 1,8 million d'assurés américains ont été victimes de fraudes identitaires. Ces vols d'identité médicale sont à la fois coûteux pour l'assurance sociale et dangereux pour la victime qui court de graves risques : mauvais diagnostics, prescriptions erronées et remboursements retardés. Les cas sont légion. En août 2013 par exemple, un cadre du principal système de santé de l'Illinois se fait voler un ordinateur portable contenant les données personnelles de 4 millions de patients. Ce même été, un vol analogue permet à ses auteurs de récupérer des dizaines de milliers de données d'assurés, non seulement leurs noms, adresses, date de naissance, taille, poids, mais aussi tous les éléments figurant dans leurs cartes de paiement, jusqu'au modèle de leur voiture.

# Le pillage du fisc

Autre victime majeure de la fraude identitaire, le fisc américain, qui a été lésé de 4 milliards de dollars en 2012. L'année suivante, il a diligenté 1 492 enquêtes pour ce type de fraudes, soit 66 % de plus qu'en 2012. En 2013 toujours, les services d'inspection fiscaux ont repéré 14,6 millions de déclarations et demandes de remboursement frauduleuses ou suspectes et ils ont bloqué pour 50 millions de dollars de restitutions indues depuis 2011. Parmi elles, 655 demandes de remboursement à une seule adresse en Lituanie et 343 à une seule adresse de Shanghai…

Au premier semestre de 2013 enfin, on estime que 1,3 million de contribuables américains ont vu leur identité dérobée. Pour la plupart, après

qu'ils ont été repérés et ciblés sur des réseaux sociaux. Plus largement, des sondages montrent qu'en avril 2014, 18 % des adultes américains utilisant Internet ont eu « d'importantes données personnelles » volées, soit 7 % de plus qu'en juillet 2013.

Les autorités concernées de Washington estiment que, pour la période 2014-2019, les demandes frauduleuses de remboursement s'élèveront à un total de 21 milliards de dollars. D'autant que, jusqu'à présent, les applications fiscales américaines pour téléphones portables se révèlent simples à pirater. Le paiement des impôts et taxes en ligne se généralise en effet Outre-Atlantique où l'on a compté 125 millions de déclarations en ligne en 2013 (deux fois plus qu'en 2012). La fraude consiste donc à adresser au fisc, le plus vite possible lors des ajustements de fin d'année (pour prendre de vitesse le vrai déclarant), des demandes par Internet de remboursement pour des taxes et contributions diverses, prétendument trop payées. L'individu qui effectue la demande est bien entendu un clone que l'ordinateur du fisc considère comme authentique. Son nom et numéro de sécurité sociale sont exacts, mais le compte bancaire du clone est contrôlé par le pirate qui disparaît dès le virement reçu.

À la seule agence fiscale fédérale américaine, 3 000 fonctionnaires combattent déjà ce type de malversations. Résultat : 165 inculpations en 2011 et 1 050 en 2012.

# Les trafics factices sur Internet

Si un site parvient à établir qu'il est très fréquenté et, pour le dire autrement, qu'il suscite un trafic intense et régulier de visiteurs de préférence jeunes, le marché de la publicité a des chances de s'y intéresser. De 2012 à 2013, le commerce en ligne a augmenté de 15 % aux États-Unis, pour un montant estimé à 42 milliards de dollars. D'où l'intérêt de multiplier le nombre de clics pour accéder à cette manne, quitte à inventer de faux visiteurs. Des Botnets proposent ainsi mille « visites » (ou « Ghost Clicks ») sur un site pour un dollar. Certains Botnets spécialisés dans ce genre de truquages sont très sophistiqués et vont plus loin que le simple « clic » : le client fantôme « visite » le site sans hâte, s'arrête sur les publicités, regarde une vidéo, place des objets dans le panier d'achat en ligne, etc. Par jour, un Botnet rassemblant environ 1 000 ordinateurs-

zombies se loue 200 dollars par jour en Russie, 180 dollars aux États-Unis et 240 dollars en Grande-Bretagne.

En mars 2013, un cyber-gang de 7 individus spécialisés dans la fraude à la publicité en ligne a été démantelé. Il contrôlait un Botnet de plus de 4 millions d'ordinateurs, disséminés dans une centaine de pays (dont 120 000 aux États-Unis) et venait de réaliser un profit de 14 millions de dollars en un an. À l'été 2014, on a appris que 23 millions de comptes Twitter actifs étaient automatiquement alimentés par des bots et que les tweets émis par ces usagers factices pouvaient constituer jusqu'à 25 % de l'ensemble. Plus largement, 30 % du trafic publicitaire mondial serait généré par des armées d'ordinateurs asservis, alimentant des dizaines de milliers de sites aux visiteurs douteux ou faux. En 2013, cette fraude aurait coûté 10 milliards de dollars à la profession publicitaire.

## Les fausses publicités

C'est un tsunami : en 2013, Google a dû retirer de ses sites 350 millions de publicités dangereuses, contre 220 millions l'année précédente. Un million environ de ces publicités « éclosent » ainsi chaque jour comme, par exemple, celles visant à attirer les internautes vers les pharmacies en ligne vendant des médicaments factices, dangereux ou contrefaits. Chez Google toujours, 270 000 « publicitaires » douteux sont interdits de séjour, ainsi que 200 000 sites illicites.

## Toujours et encore, le Spam

Spammer un géant du Net peut rapporter gros. Sur Facebook, par exemple, le Spam rapporte de 87 millions à 390 millions de dollars par an. Et sur Twitter, de 40 millions à 360 millions de dollars. Plus largement, une industrie illicite comme la vente en ligne des adjuvants sexuels (faux Viagra, etc.), surtout effectuée par le biais du Spam, rapporte à des pirates russes et indiens, en grande majorité, quelque 300 millions de dollars par an. Parmi les grands professionnels de ce marché, on trouve le Botnet russe Festi/Topol qui, parfois, expédie à lui seul un tiers de tout le Spam planétaire et contrôlerait un cinquième de ce marché pour un chiffre d'affaires estimé à 60 millions de dollars par an.

# LA FACE NOIRE DU COMMERCE ET DES SERVICES EN LIGNE

Voyons dans le détail ce que le « professionnalisme » et la « sophistication » évoqués plus haut signifient pour les sites implantés dans le « web profond ».

## Une formation en ligne au piratage toujours plus professionnelle

Un excellent service de formation, un suivi et une assistance en ligne de qualité ou une clause de remboursement en cas de non-satisfaction, tels sont quelques-uns des services proposés par des sociétés criminelles en ligne spécialisées.

Voici, par exemple, comment fonctionne un site de formation au piratage en ligne : constamment suivi et épaulé, l'« étudiant » y progresse en douceur, du cours de base sur la fraude en ligne (spécialité : fraudes aux cartes de crédit), aux cours avancés sur les outils d'anonymisation, les Botnets, l'effacement des preuves électroniques ; sans oublier, l'art d'égarer la justice.

À 75 dollars le cours, l'« étudiant » en a pour son argent. D'autant plus que ces cours sont illustrés par des vidéoconférences sur Skype où le « professeur » répond directement à toutes les questions techniques que ses « étudiants » lui posent. Au programme : comment cacher ses traces, comment contourner les antivirus et autres coupe-feu, comment utiliser les proxies (serveurs relais) des navigateurs, les boîtes courriels sécurisées et autres courriels jetables pour rester anonyme sur Internet. Seul obstacle : à ce jour, la plupart des cours en ligne les plus performants et appréciés sont en langue russe…

## Cybercommerce illicite : tout pour le client

Du fond du Dark web, des hébergeurs/fournisseurs d'accès criminalisés proposent aux « boutiques criminelles » voulant s'installer chez eux une gamme de services illicites en tous genres, les « crime-friendly e-shops ». L'un de ces hébergeurs abrite ainsi plus de 2 500 cyberboutiques criminelles

avec, pour les néophytes, une intéressante interface pédagogique leur permettant de créer aisément leur commerce. Pour un coût de 10 dollars le mois d'hébergement. En prime, le système du site (son architecture) est garanti « bulletproof » (impénétrable). Sur une sorte de tableau apposé à l'entrée du cyber-« centre commercial », les pirates hébergés présentent (en russe…) leurs « spécialités » ou proposent à la vente le produit de leurs vols.

## Silk Road, un eBay criminel au cœur du Dark web

Silk Road est un site du Dark web hébergé sur le réseau TOR. C'est à l'origine une place de marché en ligne pour produits illégaux, lancée en janvier 2011, avec pour spécificité de garantir l'anonymat à ses usagers, toxicomanes et dealers. Sur Silk Road, le « dealer 2.0 » opère depuis un café ou son domicile avec une tablette ou un smartphone. Le consommateur, lui, n'a qu'à ouvrir une boîte postale et un compte en bitcoins pour s'approvisionner. La marchandise est livrée à domicile, par colis postal, Silk Road jouant le rôle de tiers de confiance et ne débloquant le paiement que si l'acheteur est satisfait et lui communique son accord.

Cet « eBay de l'illicite » ne propose pas tous les produits illégaux. Il refuse la pédopornographie, la fausse monnaie et le recel de vol. Mais on y trouve tout le reste : stupéfiants (cocaïne, héroïne et opioïdes, LSD, etc.), faux documents d'identité, contrefaçons diverses, armes, logiciels de piratage, recrutement de tueurs à gages, etc. Toutes les transactions s'y effectuent en bitcoins et restent (en principe) anonymes et intraçables.

À l'automne 2013, le propriétaire et gestionnaire de Silk road, connu sur Internet comme « Dread Pirate Roberts » (un loup de mer, héros de romans d'aventure) est identifié par le FBI : il se nomme Ross William Ulbricht, jeune ingénieur et physicien jusqu'alors parfaitement inconnu. Il est arrêté le 1er octobre 2013 dans une bibliothèque publique de San Francisco, avec son ordinateur portable pour unique tour de contrôle et centre de gestion de Silk Road.

De son origine à son démantèlement, Silk Road a réussi à agréger une clientèle d'un million de visiteurs réguliers et a réalisé un chiffre d'affaires de 1,2 milliard de dollars, sur lequel « Dread Pirate Roberts » a prélevé un profit d'environ 80 millions de commissions (dont la police n'a ultérieurement retrouvé qu'une partie). Depuis, la répression s'est abattue

sur l'environnement de Silk Road : un vendeur de bitcoins a été inculpé et incarcéré pour blanchiment, car il savait que le million de dollars en bitcoins qu'il avait vendu à des usagers de Silk Road avait un usage illégal. Un des plus gros « commerçants » opérant sur Silk Road a été également identifié et arrêté : c'est un jeune Néerlandais de 23 ans, ingénieur en informatique. Se faisant appeler « Supertrips », il avait, avec un téléphone, un ordinateur portable et un sac à dos, vendu en dix-huit mois 566 000 cachets d'ecstasy, 4 kg de cocaïne, etc. à des toxicomanes du monde entier. Et amassé plus de 3 millions de dollars en bitcoins de bénéfice.

En novembre 2013, un mois après que Silk Road.1 a été frappé, Silk Road.2.0 est en ligne. Trente mois d'enquête du FBI ont eu pour résultat un seul mois d'effet concret. Silk Road.2.0 fait le même « métier » que son prédécesseur, mais avec un niveau supplémentaire de codage avec une clé spécifique PGP, Pretty Good Privacy, un efficace système de cryptage.

À l'été 2014, combien de Silk Road opèrent dans le dark web ? Des dizaines sans doute. Ainsi se centralise et se consolide – pour l'instant, dans l'impunité – le cybercommerce criminel.

1. Champs Flammarion, 2001.

## CINQUIÈME PARTIE

# À L'HORIZON 2020, TROIS QUESTIONS MAJEURES

Les questions que posent et se posent les organisations internationales, les géants du net ou qui mobilisent l'opinion sont décisives et stratégiques. Les réponses qu'elles susciteront détermineront les politiques à venir, à l'intérieur des États et entre ceux-ci. Ces questions sont les suivantes : quelles seront les limites au cyber-espionnage ? Des guerres numériques et du terrorisme par Internet sont-ils envisageables ? Qu'appelle-t-on prédire ?

# DOCTEUR FOLAMOUR : LA NSA ET LE PIRATAGE D'ÉTAT

En juin 2013, une rafale de *scoops* dans le *Guardian* et le *Washington Post* révèle au monde l'existence du dispositif Prism, créé en 2007 et dont l'austère matricule technique est US-984XN. Rapidement, une opinion mondiale médusée comprend qu'il n'y a pas que Prism. Chaque jour, grâce à un appareillage démesuré, la NSA peut accéder à la plupart des données téléphoniques de son choix, fixes ou mobiles, et capter, stocker, exploiter et conserver les voix, textes, courriels, Internet, chat, du monde entier, États-Unis inclus. Et ce, pour tout un chacun, du passant anonyme à certains dirigeants politiques, même alliés. Depuis 2006, tout téléphone fonctionnant aux États-Unis voit ses métadonnées* aspirées par la NSA et stockées durant cinq ans. Ainsi toute la vie privée, même la plus intime, de tout individu installé aux États-Unis est-elle espionnée par la NSA, même si sa supposée « cible » n'a absolument rien à voir avec le terrorisme.

Un tiers de toutes les communications téléphoniques, 80 % des câbles sous-marins en fibres optiques de transport de données, et 90 % du trafic d'Internet mondial transitent par les États-Unis. Les interceptions de la NSA captent tout, soit, tous programmes confondus, 20 milliards de communications par jour. Les localisations géographiques GPS des téléphones portables et les informations personnelles émanant de leurs applications mais aussi toutes les informations mondialement collectées par Google, Yahoo !, Verizon, AT & T, Microsoft, Facebook, etc. sont stockées. Le dispositif de la NSA se répartit ainsi : UPSTREAM intercepte le contenu des câbles transcontinentaux en fibres optiques ; PRISM siphonne le contenu des grands de l'industrie américaine des télécoms : AT&T, Verizon,

Sprint (à eux trois, 81 % du marché) ; SHELLTRUMPET, MOONLIGHTPATH, SPINNERET collectent les métadonnées des communications internationales ; BOUNDLESS INFORMANT siphonne et analyse les milliards d'appels téléphoniques et de courriels d'Américains aux États-Unis (pour un seul mois de 2013, selon Snowden, 3 milliards d'appels et courriels interceptés) ; X-KEYSCORE suit ses cibles en temps réel quand celles-ci naviguent sur Internet, visitent des sites ou des réseaux sociaux, font des recherches sur des moteurs de recherche ou se livrent au « chat » avec une connaissance.

## De la cyber-boulimie à la cyber-mégalomanie

S'agissant d'abord des citoyens ou résidents américains, cet effarant dispositif (et sans doute bien pire, qu'on ignore encore) permet à la NSA d'accéder à tout ce qui figure sur un ordinateur ou sur Internet. Quiconque fait un achat, téléphone, use de son compte bancaire, passe devant une caméra de surveillance, reçoit de son médecin une ordonnance, récupère ou expédie un colis, envoie un courriel, remplit une feuille d'impôts, demande un crédit, entre dans les bases de données des ordinateurs de la NSA. Ces interceptions sont effectuées sans qu'à l'origine de la captation nul lien même ténu ne soit censé exister avec quelque péril que ce soit, avéré ou hypothétique.

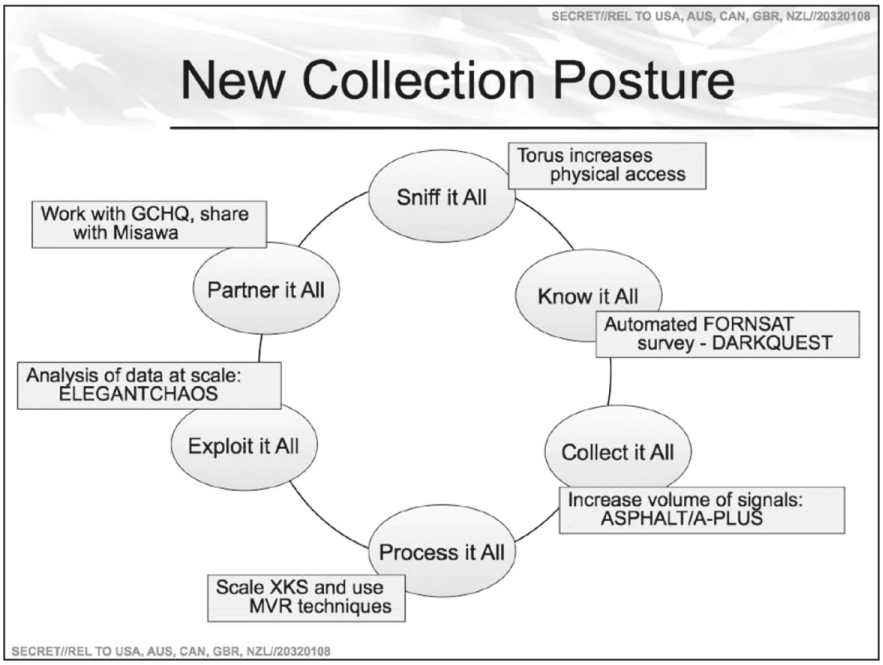
Ce qu'en fait la NSA intercepte, l'objet même de sa surveillance globale, est tout simplement la vie humaine… Phénomène particulièrement inquiétant, et c'est un euphémisme, pour les libertés individuelles et publiques. Louis Aragon écrivait jadis dans un poème, *Rencontre, partance hâtive*/*Est-ce ainsi que les hommes vivent*/*Et leurs baisers au loin les suivent*/*Comme des soleils révolus.* Eh bien, sur ces « soleils révolus » que tout homme ou femme habitant cette planète porte en lui, la NSA peut désormais et inutilement tout savoir.

Jamais d'ailleurs la NSA n'a justifié pourquoi elle opérait ainsi, ni suivant quelle logique ou nécessité. Son raisonnement semble cependant répondre à l'impératif de la lutte antiterroriste et elle s'arroge ainsi le droit de tout espionner. Son mode opératoire lui permet de cibler un numéro de téléphone qu'elle croit suspect (*seed number*) et de surveiller ensuite tous les numéros, même les plus anodins, qui lui sont reliés, puis ceux de tous les contacts téléphoniques de ce second niveau. Exemple : quelqu'un

appelle son cousin qui, la veille, a été appelé par un livreur de pizzas, dont le beau-frère a, dix ans auparavant et en Uruguay, flirté avec une militante Tupamaro, et il se retrouve *ad vitam aeternam* dans la base « suspects de terrorisme » de la NSA. Ainsi, les 300 enquêtes d'une année permettent-elles vite d'atteindre les 120 millions de téléphones espionnés… De fait, en un mois de l'année 2013, la NSA/Global Access Operations a-t-elle intercepté 124 milliards d'appels téléphoniques et 97 milliards de courriels. Soit, en moyenne, 4 milliards d'appels et 3,2 milliards de courriels récupérés par jour.

Si la « lutte antiterroriste », la pédophilie et le crime organisé peuvent expliquer une telle boulimie, celle-ci suscite une réprobation générale. En février 2014, le Parlement européen condamne fermement « le recueil à grande échelle, systématique et aveugle, des données à caractère personnel de personnes innocentes, qui comprennent souvent des informations personnelles intimes… La lutte contre le terrorisme ne peut en aucun cas justifier l'existence de programmes de surveillance de masse non ciblés, confidentiels, voire illégaux ».

De la boulimie, on descend vite dans ce que la psychiatrie qualifie de « délire d'omnipotence ». En témoigne le document Snowden (*cf. fac-similé*, source : fawww.glenngreenwald.net) qui, en 2011, expose aux *Five Eyes* (CIA et services secrets du Royaume-Uni, du Canada, d'Australie et de Nouvelle-Zélande) la nouvelle politique de collecte de la NSA : « Tout collecter – tout analyser – tout exploiter – tout partager – tout détecter – tout savoir ».




Cet objectif est très concrètement à portée de la NSA : selon un lanceur d'alerte interviewé par *The Guardian* en juillet 2014, la NSA pourra bientôt « filtrer » la totalité du trafic mondial d'Internet, soit environ 966 exabytes dans l'année, un exabyte étant égal à $10^{18}$ bytes. Commentant ironiquement les récents échecs de la NSA qui semble avoir aussi bien « manqué » l'invasion de la Crimée par la Russie que celle de l'Irak par l'« État islamique », le lanceur d'alerte affirme que, pour les États-Unis, « le but ultime de la NSA est le contrôle total de la population ».

De fait, il semble plus aisé de contrôler toute l'humanité – mais pourquoi ? – que des individus dangereux. Depuis 2008, en effet, divers islamistes, terroristes eux-mêmes ou espions à leur service, ont ainsi pu circuler aux États-Unis sans être inquiétés, voire multiplier les allers-retours avec de dangereuses zones de front sans que nul ne s'en avise à la NSA ou ailleurs à Washington. Quelques exemples ?

En 2008, « David Headley », un Pakistanais (dont le nom d'origine est Daood Sayed Gilani) vivant à New York, censé être un informateur de la DEA mais en réalité un espion de l'entité terroriste pro-taliban « Lashkar-e-Taiba » réalise tous les repérages précédant la tuerie de Bombay (novembre 2008) provoquant 173 morts et plus de 300 blessés. En

mai 2010, Faisal Shahzad, un Pakistanais, entraîné dans des camps talibans, se rend sans encombre à New York et fait exploser une voiture piégée à Times Square. Plus récemment, en mai 2014, Moner Mohammad Abusalha, né en Floride et fan de basket, meurt « en martyr », en se faisant exploser en Syrie, dans un camion d'explosifs. Entraîné au terrorisme dans les camps du Front jihadi al-Nosra, il avait auparavant fait deux allers-retours en Floride pour voir sa famille sans être vraiment détecté.

Malgré ces succès modestes dans le domaine du « tout savoir sur tout et tous », la NSA n'est pas seule dans la course : depuis l'été 2014, le FBI dispose d'un système opérationnel de reconnaissance faciale contenant 52 millions de dossiers constitués de photos d'identité judiciaire, ou issues des archives des services de renseignement, mais surtout de millions de quidams n'ayant rien à voir, de près ou de loin, avec le terrorisme et le crime organisé.

# Aujourd'hui l'Amérique, demain, le monde

Il n'est pas possible de tout détailler ici des entreprises de la NSA mais deux programmes, récemment dévoilés par des sources Snowden, montrent que l'objectif avoué de la NSA, « tout savoir », n'est pas irréaliste. Ainsi, le programme BULL RUN permet de casser la plupart des codes et des sécurités du cybermonde. Nulle limite en la matière pour la NSA, qui peut stocker toute communication cryptée tant qu'elle le souhaite, le temps de l'étudier, de la comprendre et de la décoder. Elle a ainsi contourné ou forcé la plupart des logiciels de codage qui protègent les géants du commerce et de la finance sur Internet comme les codes d'accès aux secrets des affaires, de la recherche scientifique, aux secrets médicaux, etc.

Le programme QUANTUM – une « computer network exploitation »* –, permet à la NSA (associée au Cyber command du Pentagone) de pénétrer des ordinateurs, portables ou de bureau, et aussi des Smartphones non connectés à Internet. À cet effet, la NSA a dispersé dans le monde quelque 100 000 ordinateurs équipés pour la surveillance ou la cyberguerre. Quantum vise les alliés des États-Unis aussi bien que la Chine, la Russie, l'Union européenne, l'Arabie Saoudite, l'Inde, le Pakistan, et les cartels mexicains.

Par voie de corruption, de complicité, d'infiltration humaine, etc., Quantum implante secrètement, dans des ordinateurs cibles, des

programmes permettant d'y glisser ou d'en exfiltrer des informations, par radio-transmission. Le vecteur d'infection consiste souvent en de fausses clés USB équipées de microsystèmes émetteur-récepteur. Il suffit d'une station relais contenue dans une valise (rayon d'action, environ 10 km) pour récupérer, ou y implanter, ce qu'on veut dans l'ordinateur.

Sur tout ce qui précède, les dirigeants successifs des États-Unis ont menti, et mentent toujours, à l'instar de George W. Bush qui déclarait en 2004 : « Il faut un acte de justice pour toute écoute téléphonique » ce qui était bien sûr totalement faux. En mars 2013, James Clapper, directeur national du renseignement fait devant le Sénat un effort de franchise en disant : « Je vous réponds le moins mensongèrement possible ». En matière de cyber-espionnage ou de cyberguerre, la transparence n'est donc pas pour demain…

# Les pirates pour modèles

Mais pourquoi se borner à du piratage de bonne facture quand on peut accéder aux techniques des hackers ? Dans son humour particulier, le FBI appelle cela « Going Dark », par proximité avec l'expression « Going Black » employée pour désigner une femme blanche prenant des amants Afro-américains. « Going Dark » consiste à utiliser un des logiciels (*spyware*) récupérés sur le Dark web et à l'installer sur des téléphones ou ordinateurs grâce à des courriels, ou des fichiers infectés. Une fois en place, le logiciel espion activera à distance le micro et/ou la caméra de l'appareil cible à l'insu de son propriétaire.

# D'inquiétants partenariats public-privé

Le mélange des genres entre organismes officiels et hackers finit par inquiéter sérieusement les plus lucides des experts en sécurité informatique qui dénoncent, en la matière, une dangereuse contamination. Aujourd'hui, observent-ils, ces programmes sont ceux, encore secrets, de la NSA ; demain, ils seront à la base de thèses de doctorat ; après-demain, banalisés, ils deviendront des outils pour hackers.

Piégés, « retournés », ou soudoyés, certains pirates deviennent aussi de purs mercenaires, combattant au service d'un État contre d'autres États. Or ces pirates, les vrais et les récupérés, ont pour passion la recherche des

trappes secrètes de pénétration placées par la NSA dans les logiciels de sécurisation de tous types (entreprises, services, particuliers…) – et se les échangent, ou se les vendent entre eux.

Autre problème, celui des allers-retours entre la recherche et l'administration, le public et le privé. Là aussi, les « fertilisations croisées » ne sont pas toutes positives. Dans la Silicon Valley, des anciens du Pentagone, de la NSA ou de la CIA créent des startups spécialisées dans la sécurité informatique. En 2012, de telles « jeunes pousses » ont reçu 1 milliard de dollars de financement provenant du capital-risque, deux fois plus qu'en 2010. À l'inverse, le Pentagone recherche constamment des programmeurs doués pour renforcer ses équipes travaillant sur ses programmes de cyber-espionnage.

Résultat : la plupart des outils et protocoles illicites de la NSA ou du GCHQ (son homologue britannique) finissent par être accessibles au secteur privé de la cyber-sécurité, lui-même peu régulé ni contrôlé à l'exportation. Au point qu'en juillet 2014, le nouveau Chief Information Security Officer d'un grand distributeur américain déclare, désabusé et inquiet, « tous les outils mêmes que les États ont utilisés pour des (cyber) attaques ont été mis sur le marché et sont en vente comme de simples marchandises, au marché noir ».

À Dubaï, Prague, Brasilia, Washington DC, Kuala Lumpur, Paris, Londres, etc., des salons spécialisés proposent d'ailleurs régulièrement à une clientèle officielle ou privée, ces bijoux de l'espionnage high-tech.

De fait, des entreprises spécialisées (américaines, britanniques, israéliennes, françaises, allemandes) proposent à tout État solvable – pas toujours les plus respectables – des dizaines de dispositifs d'espionnage électronique et autres technologies de surveillance/analyse supposés travailler au plus proche du temps réel. Certains d'entre eux interceptent jusqu'à un milliard de messages par jour et en stockent plusieurs milliards. Contournant désormais leurs fournisseurs d'accès nationaux par lesquels ils devaient précédemment passer pour espionner leurs clients, ces gouvernements, ministères ou services disposent ainsi de systèmes siphonnant et lisant des millions de courriels, de SMS, d'échanges par téléphone ou réseaux sociaux. Avec un dictionnaire de mots-clés, les « contrôleurs » de ces services peuvent suivre toute l'activité d'un individu cible à partir d'une simple adresse courriel ou d'un numéro de téléphone.

*Quatre questions simples*

# À quoi ça rime ?

Ne soyons pas naïfs. Plus que de permettre de déjouer le prochain 11 Septembre, cet immense dispositif de surveillance sert d'abord à intimider le citoyen lambda. Celui-ci saisit confusément que, s'il veut être laissé en paix, il doit éviter de provoquer « Big Brother » de trop près. Cela instaure en douceur un climat qui incite à la passivité, à l'obéissance et à la conformité, ce qui ne peut que satisfaire l'État qui l'a mis en place.

Pour les sociétés commerciales actives dans le cybersphère, l'inquisition numérique américaine est plus agressive. En 2013, deux fournisseurs d'accès américains offrant des systèmes de courriels inviolables reçoivent l'ordre secret de fournir des trappes d'accès aux services officiels de leur pays et donc d'accepter de dénoncer leurs clients. Par loyauté envers ceux-ci, les deux entreprises en question ont préféré détruire leurs serveurs. Aujourd'hui encore, elles sont sous injonction judiciaire formelle, lourdes sanctions à la clé, de garder le silence sur toute l'affaire. « J'aimerais, dit l'un d'entre eux, vous expliquer pourquoi j'ai pris cette décision ; mais légalement, je ne le peux pas », ajoutant « je conseille fortement à toute personne soucieuse de protéger ses données, d'éviter tout fournisseur opérant aux États-Unis ».

Autre utilité de la NSA : l'espionnage économique des rivaux des États-Unis (alliés ou adversaires). Une fuite révèle ainsi que la NSA « rend service à ses usagers » (*serving our customers*), qui sont notamment le haut représentant américain pour le commerce extérieur, les ministères de l'Agriculture, de l'Énergie et du Commerce.

# Combien ça coûte ?

Depuis l'affaire Snowden, nous connaissons le budget consacré aux cyber-opérations offensives et défensives des États-Unis. Total pour l'année fiscale 2013 : 52,6 milliards de dollars, soit 14,7 milliards pour la CIA, 10,8 milliards pour la NSA et 10,3 milliards pour le National reconnaissance office (NRO, imagerie satellitaire). À quoi il faut ajouter les 23 milliards du renseignement militaire. Pour la NSA, à qui il arrive de

conserver parfois durant un mois toutes les communications de pays entiers comme l'Afghanistan, les frais de stockage (informatique, électricité, espace numérique dédié, sécurité, etc.) sont considérables. Selon une estimation, le stockage de 5 pays pendant un an coûte 25 à 30 millions de dollars, soit des milliards de dollars par an pour tous les pays « intéressants » de la planète.

# Est-ce efficace ?

Pas vraiment si l'on en croit l'extrait du rapport du Privacy and civil liberties oversight board : « Nous n'avons pas identifié d'épisode menaçant pour les États-Unis, dans lequel le programme d'écoutes téléphoniques [de la NSA] ait eu quelque utilité que ce soit pour une enquête antiterroriste. Nous n'avons pas non plus connaissance d'un seul complot terroriste inconnu découvert grâce à ce programme ; ni de quelque attentat terroriste clairement déjoué grâce à lui ».

Un second rapport sur l'efficacité des programmes de la NSA est tout aussi révélateur : « Notre inspection suggère que la surveillance des métadonnées téléphoniques n'a pas fourni d'informations cruciales aux systèmes de prévention des attaques terroristes… » Tout cela, on a aisément pu le constater dans l'attentat de Boston, lors duquel Prism et toute la cyber-nébuleuse NSA n'ont strictement servi à rien, ni avant ni après. Pas plus d'ailleurs, pour être complet sur ce point, que les fameuses *watch lists* (listes de vigilance) du FBI, du nom de TIDE (Terrorist Identities Datamart Environnement) ou de TSD (Terrorist Screening Database), avec les centaines de milliers de fiches et de noms qu'elles contiennent ; listes où l'on retrouve en vrac, dans les dossiers électroniques de la plupart des cibles, « des prescriptions médicales, des cartes de supermarché, des contraventions pour excès de vitesse, plus des informations sur les chiens des cibles, leur assurance santé, leurs matériels de plongée, voire le contenu de leurs poches », au total un bazar si chaotique et confus que, visiblement, nul ne s'y retrouve plus.

Notons pour conclure que, de façon normale car symétrique, si les listes des personnes suspectes enflent et métastasent en tous sens, celles des « good guys » augmentent tout autant. Selon un « lanceur d'alerte », le nombre des Américains possédant une habilitation de type « très secret » approcherait aujourd'hui le million…

## Pourrait-on faire autrement ?

Certainement : la société de l'information n'est pas condamnée à pécher au chalut dans l'océan illimité des métadonnées. Dans un domaine voisin, par exemple, d'efficaces programmes permettent désormais de retrouver dans les égouts des traces de stupéfiants ou d'explosifs. Quand ces traces sont significatives et récurrentes, une enquête approfondie vise le pâté de maisons alimentant l'égout, et se borne à y cibler le seul appartement suspect.

Cette recherche « microchirurgicale » ne perturbe pas tout un quartier, voire une ville, pour trois toxicomanes ou deux apprentis artificiers. L'électronique high-tech doit pouvoir réaliser des outils permettant d'agir de façon aussi respectueuse de la légalité dans le cybermonde. Ces outils seraient sans doute plus efficaces que les pratiques consistant à bondir sur tout individu prononçant le mot « bombe » au téléphone, ou recherchant sur Internet une cocotte-minute pas trop chère…

# CYBERGUERRES*, CYBERTERRORISME* ?

> « Les responsables de la sécurité s'inquiètent de ce que les groupes terroristes accroissent leurs compétences en informatique, notamment leurs capacités cybernétiques offensives. Des terroristes peuvent aussi tenter d'acheter de dangereux maliciels à des États hostiles, ou des pirates sachant produire de tels maliciels. Le cybermonde est déjà dangereux : cela le rendra plus périlleux encore. »
>
> Reflections on the tenth anniversary of the 9/11 commission report

Au printemps 2013, on apprend que le Pentagone adopte un nouveau code de la cyberguerre, contenant de nouveaux protocoles et règles d'attaque et de défense. À cette occasion, le général Martin Dempsey, chef de l'état-major général des États-Unis présente les menaces cybernétiques comme un danger majeur pour la sécurité nationale des États-Unis. Pour lui, « un clic de souris peut plonger un pays entier dans le chaos. Un système informatique peut être infecté, pris en otage, blessé ou tué ». Et pour les

experts ayant rédigé les *Réflexions au dixième anniversaire du rapport sur le 11 Septembre*, « au niveau de la préparation cyber, c'est comme si nous étions le 10 septembre 2001 ».

Selon tous ces experts officiels et pour conjurer le spectre de ce qu'on présente aussi, à Washington, comme un futur « Pearl Harbour numérique », l'Amérique doit donc soigneusement préparer les cyber-conflits à venir, imaginer de nouvelles règles d'engagement, d'originales ripostes graduées, etc. L'Amérique le doit d'autant plus, soulignent ces officiels, et avec d'autant plus d'imagination que, dans le cyberespace, les lois de la guerre classique n'ont plus aucun sens, en raison de l'immense difficulté d'attribuer clairement toute attaque à un adversaire précis. C'est-à-dire d'attribuer rapidement à qui que ce soit toute agression au double sens technique et juridique du terme. Car le cybermonde est d'autant plus le royaume des tromperies que, on l'a vu, les cyber-espions, les criminels et les hacktivistes se volent, s'échangent ou s'achètent entre eux leurs « astuces », ce qui rend toujours plus complexe la distinction entre les subterfuges des uns de ceux des autres.

Car les auteurs de cyberattaques ont pour habitude de couvrir leurs traces. D'ordinaire, ils kidnappent des ordinateurs intermédiaires qu'ils interposent entre eux et leur cible. Ces *proxy-computers* à fausses pistes intégrées fonctionnent grâce à des TOR-routeurs à travers les dédales du dark web. D'où la nécessité absolue de bien étalonner les termes et protocoles en usage pour éviter de dramatiques erreurs de diagnostics. Or, dans le discours général sur les cyber-menaces, celui auquel accède le public, rien jusqu'à ce jour n'est dit précisément ni justement étalonné : les mêmes formules ou expressions désignent autant des actes malfaisants ou hostiles que d'authentiques actes de guerre perpétrés par voie électronique.

De la fraude aux cartes de paiement jusqu'au conflit militaire majeur, tout ou presque est mis au même niveau et dans le même sac par les médias, voire par les porte-parole officiels civils ou militaires. D'où, une confusion qu'il est important de dissiper.

# La première cyberguerre est passée inaperçue

> « Le monde dans sa réalité est cruel. La nature humaine est ainsi faite que certains groupes se détestent et qu'à l'intérieur même d'un groupe, il peut exister des

rivalités de pouvoir très aiguës. Refuser de l'admettre et pratiquer la langue de bois, c'est tromper son monde et se tromper. »

Entretien avec Yves Lacoste

Pendant qu'un bon nombre d'experts, de grands médias et de politiciens s'hypnotisent mutuellement sur l'hypothétique menace du jour, la vraie vie continue dans le monde réel. C'est ainsi que, dans l'ignorance générale et pas là où on l'attendait, une première cyberguerre est déjà bel et bien advenue à l'automne 2011. Plus un premier affrontement qu'une guerre, d'ailleurs, mais d'une importance majeure pour l'avenir. Car ici comme ailleurs, la sentence d'Héraclite conserve toute sa force : « L'initial est toujours le plus fort ».

Pourquoi cet épisode est-il passé inaperçu ? Parce que l'un des belligérants en cause est le puissant cartel mexicain de la drogue connu sous le nom de Zetas, et que la pratique des médias veut que le crime soit rangé dans la seule rubrique des faits divers pour en neutraliser les effets les plus inquiétants. À l'été 2011, Anonymous* commence à cibler les Zetas, en raison des massacres de civils qu'ils multiplient au nord du Mexique mais aussi de ses intimidations sur les bloggeurs et les internautes dénonçant leurs exactions.

Partant de l'idée que les Zetas sont organisés, Anonymous en conclut qu'ils disposent d'une structure, certes clandestine mais couvrant par obligation géographique un territoire de plus d'un million de kilomètres carrés, et par conséquent informatisée, donc piratable. Fidèle à sa mission (autoassignée) de cyber-justicier, Anonymous infiltre alors les serveurs des diverses polices et services spécialisés mexicains, et y siphonne quelque 200 000 courriels dont la substance permet de reconstituer, au total et après analyse, la radiographie précise de l'organisation des Zetas. Que cette radiographie soit publiée et le cartel, malgré son éminente capacité homicide, se retrouve nu, exposé au plein soleil, impuissant face à la répression officielle ; pis encore, désigné aux coups des tout aussi féroces bandes armées au service de ses rivaux.

En août 2011, première escarmouche : dans l'État mexicain de Vera Cruz, un bloggeur « trop bavard » est assassiné par les Zetas. Sur son cadavre, une affichette parfaitement explicite : « Voilà ce qui m'est arrivé pour n'avoir pas compris qu'il est malsain de balancer sur les réseaux

sociaux ». Comme le gouverneur de l'État de Vera Cruz et son entourage sont réputés corrompus et proches du cartel, Anonymous riposte par une virulente attaque DDoS, qui paralyse le site officiel du gouvernement local. Rendus furieux par cette résistance inhabituelle, les Zetas décapitent un autre bloggeur en septembre puis, au même motif, pendent encore un homme et une femme depuis un pont comme ils le font avec leurs rivaux et les agents de l'État.

En octobre 2011, les Zetas kidnappent enfin un Anonymous de l'État de Vera Cruz. Pour les hacktivistes, c'est la provocation de trop et ils ripostent immédiatement : si la libération du kidnappé n'intervient pas au plus tard le 5 novembre, ils menacent de mettre en ligne toute leur base documentaire sur les Zetas, concrètement des milliers d'informations personnelles sur les cadres Zetas et leurs familles, adresses, téléphones, etc. ainsi que celles de tous les complices repérés du cartel, des chauffeurs de taxi aux politiciens les plus illustres.

Le Mexique se fige dans l'angoisse : jamais les Zetas n'ont transigé sur quoi que ce soit depuis leur apparition. Tous les officiels envisagent avec horreur les effets en cascade d'une guerre en vraie grandeur Zetas-Anonymous sur la société civile mexicaine, déjà traumatisée par les tueries sans fin des cartels. Mais le 4 novembre 2011, les Zetas de Vera Cruz libèrent leur prisonnier tout en avertissant qu'ils tueront dix civils innocents à chaque Zeta dénoncé par Anonymous.

Dans cette bataille asymétrique entre une puissante armée criminelle du monde physique, forte de milliers de tueurs et d'un impressionnant arsenal (missiles sol-air et tanks fabriqués artisanalement) et l'impalpable et invisible cyber-force d'Anonymous, les pirates remportent la première manche. Les Zetas reculent et baissent les yeux.

# Cyber-espionnage et sabotage numérique

Il ne fait plus de doute que le cyber-espionnage et le sabotage numérique affectent gravement la sécurité nationale d'un pays et sa compétitivité économique. En 2013, le géant pétrolier BP annonce subir 50 000 attaques informatiques par jour. Une broutille à côté du Pentagone qui, lui, fait l'objet de 10 millions d'attaques quotidiennes.

En avril 2013, la Syrian Electronic Army (supposée proche du régime de Bachar al-Assad) s'empare du compte Twitter de l'agence Associated

Press et diffuse le message suivant « Barack Obama blessé dans une attaque contre la Maison Blanche ». Dans la minute qui suit, l'indice boursier Standard & Poor's 500 voit s'évaporer 136 milliards de dollars avant de revenir à son niveau antérieur dès le piratage révélé.

Qui sont les auteurs de ces attaques ? Certains pays ou groupes plus que d'autres ? La Chine est la première pointée du doigt. En 2013, le Data Breach Investigation Team de Verizon, un géant des télécoms, déclare qu'« en 2012, 96 % des attaques étatiques qu'il a enregistrées, et qui visaient des secrets d'entreprise ou de la propriété intellectuelle américaine, émanaient de pirates chinois ». L'ampleur de ces attaques devient telle qu'en mai 2014, le FBI lance des avis de recherche contre cinq officiers de l'Armée populaire de libération chinoise, accusés de piratage informatique et de cyber-espionnage industriel, après que 9 883 intrusions « chinoises » ont été repérées, uniquement dans divers systèmes informatiques fédéraux américains.

Les cibles de ces pirates chinois sont, selon le FBI, les entreprises United States Steel, Alcoa, Allegheny technologies, Westinghouse Electric et un syndicat, la US Service Workers Union. Sincèrement indignées ou feignant de l'être, les autorités chinoises renvoient alors Washington à ses propres turpitudes. Les pirates chinois semblent avoir cependant compris la leçon : à l'été 2014, un rapport fédéral américain souligne que, désormais, ils ciblent des organismes fédéraux plus modestes tels que la Cour des comptes, l'Imprimerie nationale, le Service de gestion des fonctionnaires fédéraux, à partir desquels ils peuvent plus discrètement infiltrer des entités beaucoup plus stratégiques comme le Pentagone ou la Sécurité intérieure. Toutefois, même une obscure agence peut renfermer des pépites : dans les ordinateurs de l'Office of personnel management, compétent pour tout le service public fédéral américain, les supposés pirates chinois ont ainsi pu piller les données du département de gestion des habilitations au secret-défense.

Dans un genre mixte, associant espionnage classique et numérique, les services spéciaux britanniques ont révélé le même mois que des puissances étrangères (Russie, Chine, Iran…) recrutent des informaticiens accédant à des systèmes sensibles, à des ordinateurs ou réseaux contenant des secrets de l'État ou du monde des affaires ; ou encore donnant accès à des informations stratégiques sur des dirigeants de l'État ou de grandes entreprises. Pour les services officiels, ces menaces, émanant d'individus

implantés dans des administrations ou entreprises cibles, représentent un défi croissant.

L'Iran est également accusé d'activités de cyber-espionnage persistantes et complexes, d'abord par les États-Unis. Désormais dotée de pirates informatiques capables d'égaler ceux de Russie ou de Chine, la république islamique d'Iran s'intéresserait depuis au moins 2011 à des cadres des industries américaines de défense, des représentants et sénateurs, des journalistes, diplomates et lobbyistes implantés à Washington. Au total, cet intérêt porterait sur quelque 2 000 cibles. Les pirates et « recruteurs » de Téhéran s'infiltreraient notamment dans le monde administratif et industriel américain par le canal des réseaux sociaux, Facebook, LinkedIn, YouTube ou Twitter. Mais aussi grâce à l'Internet où, comme cheval de Troie, ces services auraient créé un faux site d'information du nom de NewsOnAir.org. Dans l'industrie, les pirates iraniens ciblent en priorité le domaine de l'énergie. Plus offensivement, ils auraient également tenté de prendre à distance le contrôle des systèmes critiques d'exploitation des pipelines de Saudi Aramco et de RasGas (Qatar).

Quand on en vient à la Russie, il faut plutôt parler de cyber-sabotages, ou de cyber-émeutes comme en subissent ceux que Moscou considère comme des gêneurs, voire des ennemis.

En avril 2007, l'Estonie découvre qu'elle est victime d'un violent bombardement d'attaques en déni de service (DDoS). Ses banques, ses sites officiels, les pages web de ses médias sont paralysées plusieurs jours d'affilée. Mais pour un expert, c'est « plus une cyber-émeute qu'un assaut militaire ». En août de l'année suivante, la Georgie constate des attaques analogues lors du conflit avec la Russie : des attaques DDoS étouffent les sites officiels du pays et empêchent le gouvernement de Tbilissi de communiquer avec sa population. Même scénario en 2009, lors d'une crise douanière entre la Russie et le Kirghizistan.

À l'été 2014, la Russie et l'Ukraine sont au bord de la guerre. On apprend alors que « Snake », virus très sophistiqué et ultra-ciblé, a infiltré depuis 2012 bon nombre des ordinateurs du gouvernement ukrainien, dont ceux du Premier ministre. « Snake » a été créé en 2006 et de nombreux indices montrent que son origine est russe mais les preuves décisives manquent.

Il ne s'agit ici que d'une de ces « escarmouches numériques accompagnant des conflits réels », comme le souligne un expert. Certes,

elles ont un impact d'image et un effet psychologique non négligeable mais ne constituent pas pour autant une vraie guerre.

## La cyberguerre, la vraie ?

Pour mériter le nom de cyberguerre, une offensive devrait effectivement provoquer des morts physiques, de vrais blessés et de destructions significatives dans le monde réel. Pour citer encore le chef d'état-major général des États-Unis, une telle guerre électronique devrait par exemple et, au minimum, pouvoir « paralyser les réseaux militaires qui contrôlent le mouvement de nos troupes, les parcours de nos avions de combat, le fonctionnement de nos navires de guerre ». À tort ou à raison, les dirigeants de Washington s'inquiètent d'un risque de cette nature et une vraie guerre électronique leur paraît aujourd'hui aussi vraisemblable que plausible.

En témoigne le sondage réalisé en janvier 2014 auprès de 352 hauts responsables américains (militaires et civils de la Maison Blanche, du Pentagone, du Congrès et des industries de l'armement) pour qui la première menace pesant sur les États-Unis provient des cyberattaques et de la guerre sur Internet (45 %). Viennent ensuite le terrorisme et al-Qaïda (26 %) et la Chine (14 %).

## « Cyber-9/11 » : le risque du cyberterrorisme

Au plan théorique, le possible usage des technologies de l'information par un terroriste constitue une menace sérieuse : dans des sociétés où les voitures seront bientôt en autopilotage, un pirate pourrait prendre par exemple le contrôle d'un taxi et le précipiter sur une cible symbolique, ou kidnapper ses passagers pour faire valoir ses revendications. Toutefois, à l'heure actuelle, les experts sérieux restent sceptiques : ils font remarquer que, dans la seule langue anglaise, plus de 32 000 articles ont été écrits sur le cyberterrorisme mais que, dans la réalité, on ne compte toujours pas une seule victime d'un cyberterrorisme dont les capacités destructrices semblent pour l'instant hypothétiques.

Faute d'indications claires, la communauté des experts reste donc divisée sur le sujet. En témoigne le résultat d'une enquête auprès de 120 chercheurs de ce champ d'étude publié par la revue *Studies in Conflict and Terrorism* en mars 2014. À la question « y a-t-il déjà eu un cyber-

attentat ? », les réponses étaient : oui à 49 % et non à 49 %. Que l'Internet soit utile pour recruter et diffuser sa propagande, est une chose. Mais c'en est une autre qu'il serve d'arme létale.

# L'Europe, la France et les cyber-menaces

Début 2013, la Commission européenne et le Service européen pour l'action extérieure ont publié en commun un texte intitulé « Un cyberespace ouvert, sûr et sécurisé », le manifeste de l'Union européenne (UE) dans ce domaine. De leur côté, le Parlement et le Conseil européens travaillent à une directive visant à renforcer la sécurité des réseaux et de l'information au sein de l'Union. Tous ces efforts convergeant en une « Stratégie européenne de cyber-sécurité » dont voici les grands axes : développer une politique européenne de cyber-défense ; renforcer les moyens de prévention et d'opposition aux attaques ; développer des ressources industrielles et technologiques en matière de sécurité ; faire reculer la cybercriminalité.

En France, l'application de ce programme s'est traduite, depuis juillet 2011, par la mise en place auprès de l'état-major des armées (EMA) d'un officier général cyber-défense, poste rattaché au CPCO (Centre de planification et de conduite des opérations) en charge de la cyber-sécurité et de la cyber-protection. La cyber-défense concerne la partie opérationnelle, la cyber-protection, la partie préventive et architecturale, et la cyber-sécurité, l'objectif à atteindre. Une décision bienvenue car, fin 2013, le ministère de la Défense révélait avoir subi dans l'année 800 cyberattaques contre seulement 195 deux ans plus tôt.

L'EMA communique peu sur ce sujet, mais laisse quand même dire que ses armes informatiques sont opérationnelles et comptent « parmi les cinq ou six meilleures au monde ». Des informations sur la stratégie française de cyberdéfense sont cependant repérables dans la Loi de programmation militaire 2014-2019, votée à la fin de l'année 2013 qui prévoit un « Pacte cyberdéfense » pouvant investir jusqu'à un milliard d'euros, dont 400 millions en équipements nouveaux, et le recrutement de 400 mathématiciens spécialistes de cryptologie et d'algorithmes. En outre, un groupe de cyberdéfense associe le ministère de la Défense à des sociétés spécialisées comme Thalès (Systèmes d'information et de communication sécurisés), Airbus Defence & Space, Sogeti (Cap Gemini) et Orange-cyberdéfense.

# LE DOMAINE DU « PRÉDICTIF » : NAÏFS ET ESCROCS

Un monde merveilleux où tout est possible s'ouvre devant nous prédisent les appareils de communication et d'ingénierie sociale des gigaserveurs. L'avenir radieux d'une humanité connectée, libérée de ses pesanteurs millénaires…

## Un cyber-miroir aux alouettes

Bitcoin, la fin des monnaies et des banques, voire des États, la désintermédiation totale et des transactions à très bon marché, 30, 50, 80 milliards d'objets connectés dans dix ans, sans oublier l'impression en 3D, le séquençage de l'ADN, l'Internet devenant un « super-organisme vivant » ! On peut rêver en effet si l'on en juge les progrès de l'intelligence artificielle avec des machines bientôt capables de « converser » avec un humain, de conduire une voiture, d'exercer des tâches d'usine, même complexes. D'identifier aussi des images, sons ou objets, dans une base de données ; de reconnaître et de traduire des mots.

Au total, le monde devrait connaître une qualité de vie supérieure, une existence humaine plus sûre. Avec en prime, une débauche inouïe de richesses intellectuelles, l'accès à une supérieure sagesse…

Mais des ivresses du techno-futurisme à la réalité, il y a parfois loin. Car le monde de l'Internet – avant tout marchand, soulignons-le – sait aussi fort bien manipuler les foules et jouer sur la jobardise des naïfs. En termes pudiques, cette méthodologie propagandiste de l'attrape-nigaud high-tech est nommée « ingénierie sociétale ».

## Tout prédire, et le reste

Parmi ses pires fables figure le domaine du prédictif selon lequel des ordinateurs puissants, des algorithmes appropriés et le Big Data réunis en un dispositif approprié permettrait de prédire tout et le reste… Grâce à Wikipedia, par exemple, et à un modèle mathématique spécifique, on devrait désormais pouvoir annoncer avec précision, un mois à l'avance, le succès d'un film au box-office. Une recette également utilisable dans

l'agroalimentaire pour prédire le succès commercial, ou l'échec, des nouveaux sodas et « burgers » mis sur le marché.

Dès 2030, annoncent même certains, le monde disposera de machines à prédire (*global precognition machines*) pour nous débarrasser une fois pour toutes de tout le négatif qui nous encombre. D'ores et déjà, racontent des commerçants du logiciel, des spécialistes disposent du pouvoir « *to predict whether you're going to click, buy, lie or die* » (de prévoir si vous allez cliquer, acheter, mentir ou mourir). Selon eux, il serait possible de prédire le comportement humain, ce qui permettrait ensuite de prendre de meilleures décisions, de dissiper les risques financiers, de renforcer la santé publique, de détruire le Spam, de stimuler les ventes – et bien sûr de renforcer la lutte contre le crime.

Qu'en est-il justement de la « prédiction du crime » ? Depuis 2010 environ, de nombreux articles paraissent dans les médias papier ou électroniques du monde anglo-saxon qui racontent tous la même histoire : bientôt, il en ira du crime comme de la météo et des logiciels spécialisés comme PredPol permettront à la police de prédire les crimes.

Le système fonctionne déjà en Californie. Quand il a été testé, la criminalité constatée a baissé de 12 % et les cambriolages, de 27 %. Depuis, Silicon Valley bien sûr, les militaires, l'université, l'édition et Hollywood se précipitent sur ce nouveau marché.

Le livre *Predictive analytics for dummies* (*cf*. références) est caractéristique de cet engouement. Sur le ton de l'enthousiasme et de l'affirmation sans nuances, ses auteurs nous présentent le Saint-Graal. Mais concrètement, que contient ce livre ? Des banalités pour première année d'école de commerce. On y prolonge des courbes, rien de plus. Surtout, dans une table des matières détaillée de 7 pages, et dans un index qui en compte le double, on ne trouve rien, pas un mot, ni sur le temps, ni sur la temporalité – concepts naturellement cruciaux pour tout le domaine du « pré » (prédire, prévoir, présumer, etc.).

Ouvrage typique du genre, *Predictive analytics* ne définit jamais ce qu'est une prédiction. Car observer des comportements ou des habitudes, optimiser, prolonger les courbes, estimer des probabilités n'est ni prévoir ni prédire. Quand, dans un magasin, un vendeur voit par exemple une cliente acheter une robe de grossesse, est-il besoin de mobiliser un ordinateur géant pour lui proposer ensuite une layette ? De même, quand un lecteur commande un roman policier sur un site, faut-il un cyber-génie pour lui en

suggérer d'autres ? N'est-on pas là plutôt dans le classique « *Customers who bought this item also bought…* » des sites marchands ?

En fait, ce dispositif plutôt grossier qui prétend pouvoir donner du sens à des données diffuses, chaotiques et recueillies en vrac n'a rien de commun avec la prévision. Cas concret : avec la vitesse et la puissance de l'informatique, un logiciel trie en quatre catégories des clients du e-commerce :

A – Ceux qui achètent un produit en négligeant la publicité : laissés de côté,

B – Ceux qui n'achètent un produit qu'en l'absence de publicité : laissés de côté,

C – Ceux qui flânent sur Internet sans acheter en ligne : laissés de côté,

D – Ceux qui n'achètent rien sans publicité, mais à l'inverse, qui achètent s'ils en voient : ces « réceptifs confirmés » sont placés dans une base de données spécifique, puis bombardés de publicités.

La répétition du mot *predictive* dans le livre *Predictive analytics* veut exercer un effet hypnotique sur le lecteur mais rien n'y permet de vraiment prédire quoi que ce soit.

Après le marketing, le domaine de la stratégie : on apprend ainsi en novembre 2013 que l'armée américaine expérimente en Afghanistan un « nouveau modèle prédictif », *Global Database Events*, conçu par un professeur de sciences politiques de l'Université d'État de Pennsylvanie. Ce logiciel « recueille des nouvelles sur Internet » et « catalogue des événements, des élections locales jusqu'aux génocides ». Il en extrait des « prédictions à court et à long terme », utiles pour « gérer les crises » et « prévoir les niveaux de conflits en Afghanistan ».

De leur côté, les séries télé ont mis en scène l'analyse prédictive : récemment diffusée en France, *Person of Interest* a eu, en 2012, 14 millions de téléspectateurs en moyenne sur CBS-États-Unis. Dans cette série, « un génie de l'informatique met au point une machine capable de déjouer les attentats » qui « prédit aussi les crimes crapuleux ». Un « ordinateur intelligent et même doué d'émotions… une intelligence artificielle touchante »… Aux prises avec (notons au passage ce voisinage révélateur) « le gouvernement, la mafia, les policiers corrompus de New York », son héros « prévient – bien sûr – les crimes avant qu'ils ne soient commis ». Une ambiance, dit la critique, « à la *Minority Report* ».

Les universités américaines elles-mêmes se ruent désormais pour proposer à leurs étudiants des certificats ou Masters en analytique prédictive.

## « Prédire le crime » : ce que racontent les médias

Selon les multiples articles déjà publiés sur le thème de la « police prédictive », celle-ci « réduit la criminalité par l'analyse de données sur des crimes et le lieu de leur commission »… « S'agissant de personnes à risque, la méthode prédictive peut être efficace »… « Par voie électronique, le Maryland génère des prédictions sur les malfaiteurs placés en liberté provisoire, pour savoir qui tuera et qui sera tué »… « Des chercheurs et des policiers ont conçu des systèmes prédictifs qui, parmi les individus déjà condamnés pour homicide, prédit lesquels tueront encore »… « Grâce à des analyses informatiques sophistiquées, on peut prédire où et quand des crimes seront commis »… « Des programmes de police prédictive fondés sur des algorithmes et des données historiques, estiment la localisation et la nature de crimes futurs »…

Dans tous ces articles, on constate une forte connotation « communication » – mais pas une critique – qui les fait ressembler plutôt à une série de publicités rédactionnelles : « Le logiciel de police prédictive est deux fois plus efficace qu'un analyste humain disposant des mêmes données »… « Dans un secteur de Los Angeles, un outil de police prédictive a fait, en cinq mois, baisser d'un tiers les cambriolages »… « Dans tous les États-Unis, des dizaines de services de police ont déjà acquis de tels dispositifs ». Pour *The Police Chief*, organe de la puissante International Association of Chiefs of Police, « la police prédictive marque le début d'une ère nouvelle ».

## La « justice prédictive »

Décidément mis à toutes les sauces, le « prédictif » a également contaminé la justice. Car de fait – et fort légitimement – les magistrats s'interrogent, aux États-Unis et ailleurs : ce détenu en instance de libération risque-t-il de commettre un crime grave dans les trois prochaines années ? Ce primo-délinquant a-t-il le profil d'un multirécidiviste ? Or, d'usage, ces juges n'ont que leur expérience, ou leur flair, pour les aider. Et si des

logiciels « prédictifs » pouvaient contribuer à sélectionner les détenus avec pertinence ? Orienter les décisions des juges vers des peines avec sursis, des libérations conditionnelles, sans risque pour la société ? Bref, des logiciels peuvent-ils aider à évaluer le risque criminel futur que présente une personne jugée et à déterminer une sentence à venir : prison ferme, ou sursis ?

En d'autres termes, peut-on concevoir un système objectif permettant à la fois de multiplier les libérations conditionnelles et de réduire le nombre des récidives ? Mais également de choisir les détenus envoyés dans des programmes de réinsertion, durant la peine ou après celle-ci ? Un système qui permettrait encore de décider (dans un système de *common law*) qui reste incarcéré, et pour combien de temps, tout en détectant les jeunes détenus influençables à ne surtout pas incarcérer avec des criminels confirmés ?

Aux États-Unis, de tels logiciels « prédictifs » sont désormais utilisés par les comités d'évaluation des libérations sous condition dans une vingtaine d'États. Qu'y introduit-on pour évaluer un détenu ? Son âge, son sexe, ses antécédents ; la date de sa première arrestation, le niveau de son éducation, les infractions qu'il a commises, son comportement en prison ; souvent aussi, le casier judiciaire de ses plus proches amis et le résultat des tests psychologiques qu'il a subis ; et même, le possible éthylisme de sa mère durant sa grossesse. Ensuite, on compare le tout avec des profils analogues.

Là est le problème. Il est si grave qu'il pourrait dans l'avenir provoquer l'interdiction de tels logiciels « prédictifs » par la Cour suprême pour cause d'inconstitutionnalité. Car, pour émettre une « prédiction », ces logiciels retiennent toutes sortes d'éléments qui sont en général sans lien direct avec l'acte criminel commis par un individu, ce qui contrevient formellement avec le principe fondamental selon lequel toute sanction de justice doit uniquement dépendre de l'acte qu'un malfaiteur a commis – et non de ce qu'il est par ailleurs, ni de l'état de sa fortune.

Un précédent existe : en 1983, la Cour suprême des États-Unis a refusé de réincarcérer un citoyen de l'État de Géorgie qui venait de perdre son emploi. L'idée de la justice géorgienne était que le fait d'être au chômage rendait ce malfaiteur plus dangereux, et qu'il fallait donc résilier son sursis et le renvoyer en prison. La Cour a rejeté ce raisonnement qui, selon elle,

revenait ni plus ni moins à punir cet homme en raison d'un involontaire revers de fortune.

Que des décisions soient prises sur la base de calculs hypothétiques ou idéologiques inquiète naturellement, mais moins cependant après avoir lu l'étude intitulée *Extraneous factors in judicial decisions* (Princeton University, février 2011). Par comparaison temporelle de centaines de cas, cette étude démontre qu'en fin de matinée, des juges américains affamés condamnent bien plus sévèrement que quand ils ont déjeuné, deux heures plus tard…

Aléa informatique, aléa digestif, aléa toujours. Il demeure de tout ce qui précède que tout ce qui relève de la justice ou de la police « prédictives » repose exclusivement sur du rétrospectif : « Les modèles prédictifs analysent des données historiques… », ils reposent sur « des années, voire des décennies, de chiffres et de données criminels », etc.

C'est là que l'on découvre de redoutables problèmes conceptuels.

# Comment ça marche ?

Pour un prix de 73 000 dollars et un abonnement annuel de 45 000 dollars, comment fonctionne un logiciel de « police prédictive » ? Là encore, tous les articles évoqués ci-dessus fournissent les mêmes explications. On commence invariablement par saisir « toutes les données sur des crimes commis et leur localisation remontant à l'année XXX » ; ou bien « on analyse les dossiers d'environ 1,5 million de crimes commis de 2003 à 2012 »… Pourquoi ? Parce que « les infractions à venir seront souvent commises sur les lieux d'anciens délits ». À ce stade, le criminologue sursaute pour la première fois.

Les algorithmes maintenant. « Un nouvel algorithme moulinant des données criminelles (montre) où d'autres crimes se produiront probablement… », ou encore « l'algorithme comprend (au sens de "digère") le schéma criminel et produit une prédiction »… Ici, second sursaut du criminologue.

Preuve que l'affaire est sérieuse « ces algorithmes sont fondés sur les modèles de prédiction des séismes » ou « sur les modèles de prédiction des répliques des séismes ». Une obsessionnelle « preuve » d'efficacité qui revient, article après article. Le criminologue s'étonne ici à nouveau dans la mesure où il sait, comme il l'indiquera plus bas, que les séismes sont, à ce

jour, difficilement prédictibles, ce que nul des rédacteurs des articles en question ne s'est avisé de vérifier.

Plus prudents, d'autres cyber-futurologues évoquent, eux, la *predictive crime prevention* de l'avenir : elle fonctionnera à partir d'ordinateurs en réseaux, associés à des « capteurs sociométriques » ayant la capacité de prédire la probabilité de crimes, ou de comportements anti-sociaux. Mais auparavant, et ce n'est pas pour demain, les progrès en bio-cybernétique devront avoir permis de créer et perfectionner des ordinateurs équipés de neurones artificiels (fonctionnant comme les neurones biologiques, donc de produire de la vraie intelligence artificielle).

La « police prédictive » repose donc sur des fondements théoriques plutôt fragiles et nécessiterait des machines qui, pour l'heure, n'existent même pas… Cela n'empêche pas l'enthousiasme et d'autres pays, notamment en Amérique du Sud, se lancent dans l'aventure. Au Chili, des ingénieurs « mêlant la criminologie à la modélisation mathématique » ont entrepris de prédire en quels points de la frontière terrestre du pays, gigantesque avec ses 6 170 km, se produiraient des crimes et des migrations illégales. Au Brésil, au printemps 2014, la ville de Sao Paolo a acquis le système Detecta de Microsoft qui permet de combattre le crime en « agrégeant des données » et en « créant entre elles des associations automatiques ». Les policiers de la ville sont dotés d'ordinateurs portables, tablettes et smartphones pour accéder au système, et orienter ainsi leurs patrouilles vers les secteurs « chauds », dans un esprit préventif.

Mais pourquoi se limiter à l'Internet ? Patrouiller sur les réseaux sociaux peut aussi contribuer à « prédire le crime ». Pour le Predictive Technology Lab de l'Université de Virginie, Twitter peut en effet « prédire » certains types de crimes. Dans la revue scientifique *Decision Support Systems* de mars 2014, les chercheurs de ce laboratoire affirment que des Tweets géo-localisés (qu'on peut donc situer finement) peuvent « prédire de 19 à 25 types d'infractions : harcèlement, vols, agressions… ». Comment ? « Si assez de twitteurs annoncent vouloir se saouler dans le même secteur, alors on peut y "prédire" des infractions liées à l'alcoolisme ». Il faut en outre comparer ces analyses Twitter avec « les concentrations d'actes criminels historiquement fortes ».

L'analyse prédictive fonctionne toujours selon le dispositif suivant : *data mining* (recherches de données présentes sur Internet, mais souvent cachées) + statistiques + algorithmes sophistiqués et logiciels spécifiques

(*mining tools*) = modélisation, supposée prédire. Toutes ces opérations relèvent-elles pourtant de la prévision ? Non, comme nous allons le voir.

# Est-ce sérieux ?

Un point décisif, d'emblée, pour en juger. Aujourd'hui, et pour longtemps encore, l'incertitude, l'entropie, l'aléatoire, le désordre (au sens scientifique du terme) relèvent de l'imprévisible et de l'imprédictible. Pour le dire autrement, tout ce qui est possible à un moment donné n'advient pas nécessairement. Ce que Donald Rumsfeld, ministre américain de la Défense lors de la seconde guerre d'Irak, exprima fameusement en ces termes : « Il y a le connu-connu, le domaine de ce qu'on sait et sait savoir. Il y a le connu-inconnu, ce qu'on sait ne pas savoir. À quoi s'ajoute l'inconnu-inconnu, ce qu'on ignore sans le savoir ».

Affirmer donc que le calcul et l'observation algorithmiques permettent de modéliser ou de standardiser l'inconnu-inconnu relève de l'escroquerie intellectuelle. Car le rétroactif n'est jamais prédictif : sinon, avoir en sa possession la liste de tous les tirages passés d'une loterie ferait obligatoirement gagner au coup suivant. Qui plus est, souvenons-nous que l'informatique et la cybernétique n'accèdent qu'à l'univers du calculable, univers certes aussi immense que fascinant mais qui n'explique et ne comprend pas tout. Et que les cyber-outils ont le dangereux pouvoir de faire oublier à qui en use qu'un autre univers existe, celui de l'incalculable, de l'impalpable, de l'immatériel. Or seul ce second univers, qui prend le possible comme ligne d'horizon, est en mesure d'amener au savoir qui pressent, donc à l'avenir.

Pourquoi Oussama ben Laden devint-il le *moudjahid* que l'on connaît, et non pas l'un de ses (nombreux) frères ? Pourquoi Beethoven, né parmi sept enfants chétifs dont seuls deux survivront, devint-il un musicien de génie, lui et pas un autre ? Quel ordinateur peut répondre à cela ? C'est une banalité de le dire, mais si tout ce qu'on introduit dans une moulinette algorithmique provient du passé, il ne peut sortir du mécanisme qu'une supposition ou une hypothèse souvent maladroites, lesquelles se bornent en fait à grossièrement prolonger des courbes : les criminels étaient là hier à telle heure, ils y seront donc aussi demain.

L'incertitude ne se modélise donc pas, comme le prouve une étude publiée en juillet 2014 par Standard & Poors – Dow Jones Indices, intitulée

*Does past performances matter? The persistence scorecard*. Elle concerne les sociétés de bourse dites « actives » car spécialisées dans l'activité de « battre le marché », c'est-à-dire dans le fait de gagner sur un an et pour une sélection d'actions, plus que ce qu'un marché de référence a gagné en moyenne.

De 2009 à 2014, S&P-Dow Jones Indices analyse ainsi 2 862 de ces sociétés. Sur la période étudiée, on recherche, dans ces sociétés « actives », lesquelles sont constamment dans les 25 % des plus performantes. Réponse : deux. Deux succès, 2 860 échecs. Et, malgré les algorithmes et la communication sur les « prédictions », il apparaît que les sociétés de bourses les plus performantes d'une année sont les plus mauvaises de l'année suivante. Or, si des logiciels à base d'algorithmes spécifiques permettaient de « prédire le marché », les 2 860 sociétés de bourses en échec se seraient ruées dessus, ce qui n'est pas le cas. Pourquoi donc ce qui, toujours ou presque, échoue en matière de finances, domaine aux enjeux formidables, devrait-il réussir pour la police ?

Dès les premiers ordinateurs, l'idée de prédire a d'ailleurs taraudé les scientifiques. Au début de la Seconde Guerre mondiale, Norbert Wiener, père de la cybernétique, tenta de concevoir un modèle prédisant les évolutions des avions de chasse allemands pour pouvoir les abattre plus aisément. Ce fut un échec, par manque, dit-on alors, de capacités de calcul. Depuis trente ans et plus, la Defense Advanced Research Projects Agency (Darpa) cherche comment agréger et combiner une foule de données d'apparence déconnectées ou hétéroclites pour y découvrir des corrélations permettant de poser des diagnostics ou de faire des prédictions, par exemple sur de futures émeutes et de futurs attentats. En vain.

Récemment encore, la Darpa a lancé le programme « Data to decisions » doté d'un budget de 92 millions de dollars qui vise à concevoir un algorithme permettant de connecter, d'exploiter, de donner un sens et d'anticiper à partir des masses d'informations stockées, commercialisées, échangées dans l'Internet. Toujours dans le même but : prédire l'agitation sociale, les attaques terroristes, les événements stratégiquement significatifs. Or, à en juger par la politique étrangère américaine, de l'Afghanistan à l'Irak, la Darpa ne semble pas vraiment avoir trouvé cet équivalent prédictif de la pierre philosophale…

## Rien de moins neutre qu'un algorithme…

Comment expliquer cet échec ? Par le fait que les ordinateurs et l'informatique ne sont pas neutres. Et que les outils de collecte et d'analyse des données ne le sont pas davantage. Les algorithmes ne sont pas un étalon infaillible mais peuvent fort bien reproduire certains biais de leurs créateurs, qui ne sont que des humains faillibles et ont donc pu y instiller du *wishful thinking* dans leur travail. Pire, ils peuvent avoir été truqués par leurs créateurs (en leur faveur à eux) ; ou par des pirates. Entrevoit-on alors ce qu'il adviendrait du dispositif de « police prédictive » ainsi « arrangé » par des hacktivists du dark web ? Les patrouilles de police envoyées là où rien ne se passe pendant qu'à l'autre bout de la ville des cambrioleurs pourraient opérer en toute tranquillité ?

Plus largement, il est difficile de vérifier si des algorithmes remplissent vraiment leur tâche car, du fait de leur masse, de leur puissance même, ils influent sur la réalité et la préformatent. Si leur usage est massif, ils suscitent leur propre validité et exercent un effet « banc de poisson » sur les faits matériels.

Tout cela, les adeptes du « prédictif » devraient le savoir, d'autant plus qu'en matière de trucage d'algorithmes, les exemples récents ne manquent pas : dans la décennie 1970 déjà, le Black-Scholes Model « prédit » la valeur future des actions. Mais en 1998, algorithmes ou pas, le hedge-fund (fondé sur ce modèle) baptisé Long Term Capital Management s'effondre, poussant au bord du grouffre le marché mondial du crédit. En 2001, un modèle trafiqué fondé sur de fascinants algorithmes permet à la société Enron d'attribuer une valeur astronomique à des actifs évanescents. Puis Enron s'effondre.

Lors de la crise des subprimes, on découvre que des agences de notation « adaptent » leurs logiciels, reposant sur d'ésotériques algorithmes, au résultat souhaité. Après la crise, le géant bancaire J. P. Morgan doit « s'excuser » de l'usage d'un logiciel « inadapté », cependant fondé sur des algorithmes sophistiqués, ayant pourtant conduit la banque à perdre 6 milliards de dollars. En 2008 encore, trois importants hedge-funds subissent des pertes énormes du fait de « mouvements imprédictibles du marché ». Mouvements que les algorithmes de ces hedge-funds étaient censés prévoir…

Au-delà, les algorithmes peuvent permettre de superbes escroqueries. Dès 2005, un businessman texan, prétendument ancien officier du renseignement militaire et professeur d'université, se dit l'inventeur d'un

algorithme permettant de faire fortune sur le marché des devises étrangères. Il escroque ainsi 33 millions de dollars à ses clients naïfs, puis écope de vingt ans de prison.

Dans ces conditions, la « police prédictive » est-elle sérieuse ? Pour y répondre, revenons à l'omniprésente référence de ses « fans » à la « prédiction des séismes ». Voici ce qu'en dit le géophysicien Bill Ellsworth, chercheur à l'United States Geological Survey : « Nul ne sait prédire les tremblements de terre… Si les séismes sont prédictibles, nous ne savons pas le faire. Et ils sont sans doute vraiment imprédictibles… Nous ignorons même quelles équations régissent la mécanique des séismes… » Commentaire de celui qui l'interviewe : « Un savant comme Bill Ellsworth qui, *sans limites financières*, *[nous soulignons]* dispose de toutes les données et de toutes les capacités informatiques possibles, admet qu'il ne voit pas vraiment comment prédire les tremblements de terre ».

De même, le milieu criminel s'inscrit clairement « dans le monde réel, là où les interactions humaines complexes ne peuvent pas toujours être saisies, même par les modèles les plus sophistiqués », là où les outils d'analyse statistique tendent à produire des résultats dénués de sens. Interrogés par l'auteur, plusieurs experts en algorithmes ont fini par admettre que, dans leur conception, les logiciels de « police prédictive » étaient sans doute proches de ceux utilisés par les sites de rencontre en ligne. À leur tour, ceux-ci sont-ils, eux, sérieux et efficaces ?

Il ne le semble pas. En juillet 2014, un scandale éclate dans ce domaine. Mathématicien diplômé de Harvard, le fondateur et propriétaire du site de rencontres OK Cupid, affirme alors qu'en matière de rencontres sentimentales, « les algorithmes sont de la m… » et que dans le domaine des sentiments, « une compatibilité illusoire fonctionne aussi bien qu'une vraie ».

Où se situe donc l'astuce ? Après avoir rempli un long questionnaire (350 items), les clients d'OK Cupid attendent que la machine leur propose l'âme sœur. Or au quotidien, l'ordinateur peut fort bien annoncer à des gens incompatibles (30 % de compatibilité) qu'ils sont à 90 % compatibles. Il ne s'agit là ni de mathématique, ni d'informatique mais, côté humain, d'autosuggestion, de l'envie d'y croire, de l'exploitation d'une inépuisable crédulité et désormais, d'une absurde « foi » en les algorithmes. Et, pour le site, d'une cynique confiance en l'effet désinhibiteur d'un avis

« scientifique » sur des naïfs. Sauf que, prédit un expert, « ça se conclura sans doute par des larmes quand ils se rencontreront vraiment ».

Et pour les policiers qui ont acheté les logiciels de type PredPol, cela se conclura de quelle façon ?

## L'homme, le crime et la machine

Une remarque, banale mais qui semble échapper aux thuriféraires de Big Data : l'activité humaine n'est pas une ressource naturelle qu'il suffirait d'extraire du cloud pour la rentabiliser. Elle n'est pas une sorte de charbon ou de pétrole qu'on peut exploiter à son gré. Car l'individu, qu'il soit criminel ou non, ne se laisse jamais observer passivement. D'abord, parce qu'il n'est pas un robot mais surtout du fait que, dans ses gènes, il conserve la mémoire des millions d'années passées à fuir des prédateurs. Or l'être humain n'a pour seule arme que son cerveau ; toujours, il s'adapte, se cache, ruse ou triche, toujours, il réagit. Constamment, l'homme joue donc contre l'observateur/ordinateur. Extraire le Big Human Data n'est donc pas une simple activité minière analogue à l'exploitation d'une matière première, c'est une constante et difficile partie d'échecs, voire un brutal match de boxe contre un adversaire qui, d'instinct et toujours, évitera de se découvrir.

Dans le domaine de l'illicite, voici un exemple de ce qui précède. En France, devant la multiplication des radars le long des routes et autoroutes, les conducteurs s'adaptent en trichant. Ainsi, les usurpations de plaques d'immatriculation des véhicules explosent puisque, de 2010 à 2012, on passe de 5 079 d'usurpations à 17 479…

## De l'utilité de Big Data et de sa capacité à prévoir

Si, dans sa conception actuelle, la « police prédictive » relève de l'illusion, la voie du prédictif n'est pas pour autant bouchée. Les outils de *data mining* excellent, en effet, dans le vaste domaine du connu-connu : nul mieux que l'informatique ne sait trier, classer, ordonner – donc optimiser, à une telle vitesse. Dans le domaine de la santé, les logiciels spécialisés améliorent beaucoup les diagnostics médicaux, ou le criblage thérapeutique. Il en va de même pour le ciblage publicitaire ou l'estimation des primes

d’assurances. Dans ces domaines, un travail croisé entre experts et criminologues suscitera sans doute d’utiles outils préventifs.

L’exploration du Big Data permet aussi de discerner les tendances nouvelles, de révéler des faits sociaux émergents, d’entrevoir des dynamiques discrètes, ce qui peut se révéler précieux en matière de sécurité. Mais dans l’attente de percées technologiques majeures, aller plus loin et tout promettre pour demain matin serait à coup sûr périlleux.

# SIXIÈME PARTIE

# PRESCRIRE

Cybermenaces, cybercrime, cyberterrorisme, cyberguerres : face aux risques et périls numériques, que faire et comment faire ? Nous avons vu qu'en matière de crime, de terrorisme et d'espionnage, nulle invention propre à un cybermonde n'émergeait pour l'heure. À tout le moins, aucune ne brille par son originalité mais reste plutôt dans le domaine classique et, le plus souvent, se contente d'adapter à l'univers du cyber ce que les malfaiteurs et les espions pratiquent dans le monde physique.

Qu'en est-il donc des possibles ripostes ? Comment réguler le cybermonde – si c'est seulement possible ? Comment y encourager les bonnes pratiques et y réprimer brigandage et attaques ?

# Cette fois-ci, c'est sérieux…

Première mondiale en mai 2014 : comme on l'a vu, les États-Unis inculpent cinq militaires chinois pour cyber-espionnage. Le site du FBI affiche une mise en examen de 56 pages avec, au premier plan, les photos de ces officiers de l'Armée populaire de libération en uniforme, et le mot WANTED en capitales rouges, comme de vulgaires voleurs de chevaux du temps du Far West.

Des experts observent cependant qu'en matière de cyber-espionnage, Washington a peut-être commencé par le plus facile car, soulignent-ils, si les cyber-défenses américaines repèrent environ 80 % des attaques chinoises, ils ne détecteraient que 20 % de celles des Russes, qu'on présente comme bien plus sophistiquées. Le gouvernement chinois, on s'en doute, a démenti avec vigueur en invoquant les révélations de Snowden sur le système Prism, mais l'initiative américaine marquera l'avenir du cyberespace en matière de renseignement et, plus largement, de compétition économique.

# Le (nouveau) marché du siècle

Cet épisode annonce donc un tournant dans l'histoire d'une cyber-sécurité dont, simultanément, le marché explose. Déjà en 2013, les dépenses mondiales en la matière ont dépassé 60 milliards de dollars et elles croîtront, selon les analystes, de 6 à 9 % par an les cinq prochaines

années, pour atteindre peut-être 165 milliards de dollars en 2022. Plus englobants, d'autres modes de calcul prévoient que le marché cyber-sécuritaire représentera entre 80 et 150 milliards de dollars par an. Aux États-Unis, le seul gouvernement fédéral dépense actuellement quelque 15 milliards de dollars par an pour assurer sa cyber-sécurité.

Tous budgets publics et privés réunis (actions préventives et curatives), certains experts estiment qu'en 2013, les États-Unis ont dépensé un total de 67 milliards de dollars pour leur cyber-sécurité, et que ces dépenses devraient tripler d'ici 2016.

Considérons à présent le Cloud et sa difficile sécurisation. Tous aspects confondus, les dépenses consacrées au Cloud augmentent de façon exponentielle. Les spécialistes voient ces dépenses atteindre 210 milliards de dollars dans le monde en 2016 avec un bond de 172 % depuis 2010. La seule sécurisation du Cloud, indique en octobre 2013 le rapport Infonetics, a coûté 3,2 milliards de dollars en 2013 et elle dépassera les 9 milliards en 2017.

La fièvre de la cyber-sécurité gagne le monde des assurances dans la mesure où les grandes entreprises sont de plus en plus nombreuses à s'assurer contre les cyber-risques, en particulier celui du piratage de leurs fichiers clients. Désormais, les grands de la profession proposent des polices portant sur la responsabilité civile des souscripteurs, leurs éventuelles pertes d'exploitation, le coût d'interventions techniques internes ou externes en cas d'attaques, de possibles dommages et intérêts pour les clients et les frais de notification et de gestion d'une communication de crise, cruciale en pareil cas. Ces primes représentent 1 % du montant garanti. En 2013, les primes de cyber-assurances payées aux seuls États-Unis ont atteint 1,3 milliard de dollars contre 1 milliard l'année précédente.

# Problèmes immenses, mais immense inconscience

Cette récente prise de conscience des périls du cyber monde, cette mise en ordre de bataille de certains pays et de certaines entreprises face au piratage sont insuffisamment généralisées. Trop souvent encore, les pirates accèdent avec une désarmante facilité aux données les plus confidentielles des particuliers ou des entreprises.

Premier responsable, les mots de passe. Dans un pays aussi sensible à la cyber-sécurité que la Grande-Bretagne, où la presse multiplie sur le sujet

enquêtes et articles documentés, où le Parlement et le Gouvernement encouragent les bonnes pratiques, seuls 42 % des usagers d'Internet ont un mot de passe pour leur téléphone portable ou leur tablette. Et quand ils en ont un, ils sont désarmants de simplicité : nom d'un animal de compagnie, date de naissance, simple suite de chiffres… Début 2014, l'enquête annuelle de la société Splashdata donne ainsi la liste des mots de passe les plus utilisés dans le monde (http://splashdata.com/press/worstpasswords2013.htm). Les quatre premiers sont par ordre décroissant : 123456, password (*sic*), 12345678 et qwerty.

Pour nombre d'entreprises, la négligence est encore trop souvent la règle. On a vu plus haut les ravages provoqués par le piratage des données clientèle de la chaîne américaine de grande distribution Target. Cependant, même après ce gigantesque siphonage de données confidentielles, l'un des meilleurs experts américains de la « face noire de l'Internet », Brian Krebs – dont le site krebsonsecurity.com mérite d'être visité – souligne, désabusé, le désintérêt des entreprises pour le cybercrime, plus précisément pour le *threat intelligence* (le renseignement portant sur les menaces). « La plupart des gens, dit-il, ne voient pas pourquoi ils paieraient pour cela », à savoir pour être avertis des menaces pesant sur eux.

# ABORDER LES QUESTIONS FONDAMENTALES

## Cybermonde et monde physique : quels sont les acteurs ?

Face à Silicon Valley et aux gigaserveurs, on ne trouve que l'État. Difficile d'imaginer des forces – partenaires ou adversaires ? – plus dépareillées. D'un côté, les réseaux, le mouvant, le diaphane, le rapide, soit le cybermonde. De l'autre, l'État, l'autorité centrale, le stable, le lourd, le lent, soit le monde physique. C'est le char d'assaut contre la Ferrari. Face au cybermonde en effet, l'État est timide, maladroit, peu compétent et souvent corruptible. Il happe de-ci de-là des cyber-outils (sécurité, espionnage) qu'il adapte à son usage, mais comprend mal le cybermonde dans son principe. Et plus les choses avancent, plus les États doivent eux-

mêmes devenir des gigaserveurs pour survivre. Or c'est le domaine d'excellence des géants du net qui l'ont inventé et où leur avance est écrasante.

Même Washington peine à comprendre, maîtriser ou réguler la Silicon Valley et la cyber-finance (transactions à haute fréquence, etc.). L'État ne parvient pas ou mal à saisir la logique et les ambitions des géants du Net. Dans le meilleur des cas, il finit par comprendre, mais tard. Encore, ne parlons-nous ici que des grands États développés. Plus petits et plus faibles, les autres étant des cibles beaucoup plus fragiles.

L'État ne répond souvent que par la routine bureaucratique. Après de grandes conférences internationales comme les « Assises de la sécurité des systèmes d'information » (Monaco, octobre 2013), un observateur avisé a pu dire qu'« en France, lorsqu'on a un sujet sensible qu'on ne sait pas résoudre, on crée une commission qui produit quelques kilos de papier, qui deviennent une bible et on se dit à l'année prochaine. Bref, des sujets importants peu ou mal traités, voilà le sentiment qui nous reste de ces Assises ».

Dans ces limites, l'État a-t-il la capacité de survivre dans l'économie de l'information ou, pour le dire autrement, qui, *in fine*, dominera le cybermonde ?

## Un « code de la route » ?

C'est de l'État que procède et que provient un univers numérique qui n'est pas apparu tout seul : la génération spontanée n'existe pas plus ici qu'en biologie. Ceux qui ont fondé le cybermonde, qui l'explorent, l'arpentent et le balisent ont tous été plus ou moins proches des États. Or le passage du physique au numérique a induit et induit toujours certaines questions touchant aux *décisions*. Qui choisit ? Qui décide de numériser ou pas ? Selon quels critères ? Pourquoi ? Au profit de qui ? D'où vient l'orientation de ce qui est destiné à être numérisé ? Car l'acte même de numériser ou non, oriente. Souvenons-nous des « dictionnaires » d'Échelon, des « selectors » de Prism.

Nous allons tout numériser promettent les démiurges de Silicon Valley. Faut-il les croire sur parole ? Ne rien vérifier ni contrôler de leurs projets ? Non. Et c'est là l'éminente mission de l'État afin de nous éviter le sort de zombies décérébrés. Aujourd'hui le cybermonde, également décrit à son

origine comme une conjugaison d'« autoroutes de l'information », n'a toujours pas de code de la route digne de ce nom. Or mettre en place des codes relève du domaine régalien des États. Qu'une coalition de grands États impose un code global de l'Internet et du cybermonde, et ces États reprendront le dessus. Ils diront la loi et imposeront le droit. Ils sont les seuls à pouvoir le faire. Cela ne résoudra pas tout, notamment sur le plan des actions criminelles : les criminologues savent fort bien que les malfaiteurs fuient les codes. Quand un secteur est trop codifié, ils émigrent. Cette loi ne connaît pas d'exception : on l'appelle *effet de déplacement*. Les domaines dans lesquels émergent les nouveaux métiers criminels, internationaux – contrefaçons dangereuses, pillage des paris sportifs, etc., en témoignent : ils ont un point commun, leur totale absence de codes.

# La cyber-sécurité est-elle un problème technique ?

Pour tout technicien, la solution est nécessairement technique. La maladie est informatique ? Son traitement devra l'être aussi. Voilà pourquoi, en matière de cyber-sécurité ou de cyber-défense, seuls ou presque s'expriment des marchands de logiciels ou des VRP pour « solutions » miracle, purement high-tech évidemment. Pour les uns, tout est dans la sécurisation des « comptes à privilèges » et toutes les attaques ne sont au fond que des usurpations ou gains indus de privilèges. Le verrouillage et la traçabilité de l'accès à ces comptes assurés, les risques criminels devraient être contrôlés.

D'autres prônent une meilleure formation à la sécurité informatique des personnels des entreprises, de façon à protéger les systèmes et architectures en réseaux et à jongler avec les systèmes de détection d'intrusion. Une fois les informaticiens d'entreprise dotés du statut de *risk manager*, de *computer hacking forensic investigator*, ou de *network security administrator*, etc., la forteresse est censée devenir imprenable. Enfin, selon certains, il faut impérativement renforcer le cadre juridique et judiciaire de la lutte contre le cybercrime. Là encore, une fois ce cadre dûment renforcé, tout devrait s'améliorer.

En réalité, tout cela ne suffit pas car optimiser un *process* et réellement améliorer une situation sont deux entreprises dissemblables : construire une ligne Maginot parfaite ne garantit pas une meilleure protection contre

l'invasion. Si l'on va plus loin : est-il seulement possible d'optimiser le réel par la technique ?

## Le milieu cybercriminel est-il impénétrable ?

Non. Certaines sociétés privées de sécurité se lancent d'ailleurs dans le cyber-renseignement en utilisant de façon proactive les vieilles méthodes de l'espionnage classique comme l'infiltration d'un cyber-gang hostile. La nouvelle génération de cyber-espions nomme cette pratique le *virtual Humint* (renseignement humain virtuel). Quand elle détecte un projet hostile, une prochaine cyberattaque, par exemple, grâce à cette pratique, la société pratiquant le *virtual Humint* prévient le client visé. Dans le respect des règles de droit, il faut donc encourager la création ou le développement de sociétés privées de renseignement informatique efficaces, professionnelles et à vocation offensive.

## Les solutions de sécurité du cybermonde, réalité ou mirage ?

Les méthodes vantées par les adeptes du tout numérique pour lutter contre les criminels, les terroristes ou les escrocs financiers ne résistent pas à l'examen. On a vu plus haut que les techniques d'optimisation du travail policier, la *predictive policing*, étaient finalement loin d'être efficaces. Les deux autres méthodes d'enquêtes par voie informatique sur l'Internet, le *data-mining* et le *crowdsourcing*, le sont-elles davantage ?

Le Pr Michaël Brenner, analyste lucide et toujours bien informé, estime à ce propos que « cette méthode [Data mining] ne fonctionne pas, quelle que soit la perfection des algorithmes et matrices en usage. En l'utilisant, nous avons vainement pourchassé Ben Laden dix ans durant, et sommes rentrés bredouilles. Comme le prouve l'issue de cette traque, tout renseignement efficace exige des sources humaines et une expertise qualifiée – bien plus que des données brutes, assemblées aléatoirement. Dans un tri sélectif de données, tout indice émergent ne prend d'ailleurs sens et signification qu'à l'aide de méthodes traditionnelles. Il en va ainsi de toute action conçue comme pertinente, réalisable et ciblée ».

Le crowdsourcing est la forme numérique de la traque d'un malfaiteur ou d'un terroriste par des volontaires réunis sur divers réseaux sociaux après un attentat, un braquage ou un enlèvement. Il repose sur le constat que des millions, voire des dizaines de millions de smartphones, sont à tout instant en fonction. Des témoins d'une scène la photographient, la filment ou l'enregistrent, puis transmettent le fichier à l'autorité qui a donné l'alerte. Le crowdsourcing arrive toujours avant les équipes de télévision. Sur site, il le « couvre » plus vite et mieux que les médias. Comme il y a désormais « une caméra dans chaque poche », que des dizaines de milliers de volontaires acceptent d'aider les forces de l'ordre et que l'Internet est une formidable force de démultiplication, la traque des criminels devrait, théoriquement, se révéler plus facile.

L'attentat de Boston en avril 2013 qui a fait 3 morts et 170 blessés montre que ce n'est pas aussi simple. Dès l'explosion des deux bombes, la traque débute sur Internet. C'est l'heure de gloire du site d'échanges REDDIT, l'un des tout premiers au monde en termes de visiteurs, dont les pages vues se comptent en milliards. Des photos aidant, l'Amérique se persuade vite qu'elle « tient » le coupable et bascule dans l'hystérie en ligne. Le terroriste est à coup sûr Sunil Tripathi, 22 ans. La chasse va alors vers son issue tragique : Tripathi n'est pour rien dans l'affaire, il est en fugue depuis la mi-mars et ce « dangereux islamiste » n'est pas même musulman ! On le retrouve noyé le 23 avril dans une rivière de l'État du Rhode Island, peu après l'attentat. Un suicide consécutif à une invivable pression médiatique.

Pendant ce temps, 120 agents du FBI scrutent les 13 000 vidéos et 120 000 photos issues du crowdsourcing, et envoyées aux autorités après l'attentat. Pour rien, car ce sont uniquement la banale caméra de surveillance d'un magasin et le simple témoignage d'un blessé qui mettent finalement la police fédérale sur la piste des terroristes, les frères Tsarnaev.

Le crowdsourcing n'est pas pour autant inutile : il est déjà particulièrement efficace en mode *push* (des autorités vers le public) et permet de lancer des alertes, de diffuser des informations urgentes, de signaler des fugitifs dangereux, entre autres. En mode *pull* (du public vers les autorités), des initiatives visent à éliminer le plus possible de « faux positifs » et à éviter les chasses aux sorcières. La plus intéressante à ce jour est le système LEEDIR (pour Large Emergency Event Digital Information Repository), sorte de « baquet digital » voué à recueillir des éléments

pertinents (photos, vidéos, son) lors d'émeutes, d'attentats, de catastrophes, etc., puis de les transmettre aux autorités.

Associant une application et un espace de stockage dans le cloud, le partenariat public-privé LEEDIR, conçu par la startup CitizenGlobal et Amazon Web Services, est gratuit pour les officiels et le public. Au lieu d'inonder des messageries officielles déjà saturées lors d'un drame, toute information de type crowdsourcing est stockée, triée et transmise depuis cet espace neutre dédié.

## Au préalable, nommer, comprendre, agir

Telles sont réellement les perspectives techniques de la sécurité informatique. Elles ne suffisent pas, pourtant, à élaborer une stratégie.

Peut-on décider de sécuriser un système économique ou financier « tous azimuts » pour être sûr de ne rien manquer, au cas où ? Évidemment non. En ce domaine, le cybermonde ne diffère en rien du monde physique. Comment donc s'engager dans la bonne voie ? En partant des fondamentaux.

Dans l'ordre des priorités, le premier d'entre eux est le besoin impératif d'une réglementation légale internationale du cyberespace – le « code de la route » évoqué ci-dessus. Ici, la Russie joue un rôle important, d'autant plus que sa compétence en matière d'informatique est aussi manifeste que sa cybercriminalité est exubérante. Aux Nations unies, la première proposition russe de résolution sur la coopération nationale en matière de sécurité de l'information remonte d'ailleurs à 1998. Une proposition qui portait sur l'élaboration de règles internationales de comportement, dans le domaine de la sécurité de l'information.

Que de telles règles existent et soient acceptées par le plus grand nombre d'États est un préalable au second des fondamentaux qui, lui, concerne le fond des choses. Il nous vient du lieutenant-colonel Ferdinand Foch, alors professeur à l'École supérieure de guerre et tient en une phrase concise où chaque mot pèse lourd : « Nos forces s'engagent, s'égarent, se compromettent dans de fausses directions, en raison même de l'insuffisance de reconnaissance, du renseignement, soit de la notion de sûreté : art d'agir en sécurité comme aussi sûrement, c'est-à-dire en connaissance de cause ». La sûreté est ainsi le fait de savoir juste. Comment donc ne pas divaguer ?

Simple en théorie : il faut produire un diagnostic pertinent, ce qui revient à nommer.

Nommer, ce que nulle machine ne sait encore faire, est un impératif connu dès l'antiquité, européenne comme chinoise. L'éminent sinologue Simon Leys le souligne ainsi : « Un de ses disciples demanda à Confucius ce qu'il ferait si on lui donnait un territoire à gouverner et le maître répondit qu'il "rectifierait les noms", qu'il ferait en sorte que les mots correspondent à leur réalité. Si les mots sont incorrects et ne correspondent pas à la réalité, le langage n'a pas de sens. Si le langage perd tout sens, l'action devient impossible, et ainsi toute activité humaine périclite et toute entreprise devient futile ».

Nommer justement importe plus encore dans un contexte de risques et périls mal connus et méconnus à la fois, où l'œil expert du criminologue perce à peu près seul le brouillard des illusions et des mensonges pour y détecter les archétypes, le nouveau et le dangereux.

Dans son magistral *Classes Laborieuses, classes dangereuses à Paris pendant la première moitié du XIX*e siècle, Louis Chevalier soulignait ainsi jadis l'importance de nommer le monde ouvrier naissant qui, dans la première moitié du XIXe siècle, était alors l'entité floue et menaçante par excellence. Chevalier montre l'importance des *Mystères de Paris* d'Eugène Sue pour les réformateurs sociaux fouriéristes qui, dit-il, « ont pris conscience de leur propre condition, l'ont découverte, parce qu'ils trouvaient dans cet ouvrage les images ou les mots qui allaient désormais leur permettre de désigner les faits qu'ils comprenaient mal, impuissants qu'ils étaient à les désigner, à les nommer ».

Que font ainsi les scientifiques qui découvrent une planète, un animal, une maladie ? Ils les nomment et, dès lors, la planète, l'animal, la maladie, existent. Nommer tire de l'obscurité, de l'anonymat, nommer institue le connu. En médecine, ne pas nommer correctement une maladie, c'est rater son diagnostic et souvent, condamner le patient. De même, ne pas vouloir ou ne pas pouvoir désigner justement et à temps une entité menaçante, condamne sa cible à la guerre de retard. Ainsi surprise à cause de son propre aveuglement, la future victime potentielle devra subir, et dans de mauvaises conditions.

Pour ce qui concerne le cybercrime, nommer juste permettra d'éviter les erreurs souvent irréparables de diagnostics. Cela nous ramène à un Jaron

Lanier exaspéré par le côté besogneux, poussif et myope de tout ou presque de ce qu'entreprend la cyber-sécurité. Lanier avertit : « L'objectif à long terme d'une stratégie de sécurité ne peut être d'agir plus intelligemment que des criminels, car cela ne fera que multiplier les criminels intelligents ». Ce qui n'est bien sûr pas souhaitable. Penser la cyber-sécurité demande donc une prise d'altitude, de l'imagination et une grande capacité à prévoir. Sur l'imagination, Simon Leys toujours : « L'incapacité occidentale à vraiment comprendre la réalité soviétique, et celle des autres variantes asiatiques du communisme, relevait d'un grave défaut d'imagination ».

Valéry Gerasimov, chef d'état-major général russe, ne dit pas autre chose quand il déclare en février 2013 : « Le mépris des idées nouvelles, des approches originales, des opinions divergentes, tout cela n'a pas lieu d'être dans les sciences militaires. Il est plus inacceptable encore que des praticiens méprisent ces mêmes sciences… Ne copions pas les expériences étrangères ; ne courons pas après les pays dominants : dépassons-les et investissons nous-mêmes les positions stratégiques. Chaque guerre est unique et exige que l'on comprenne ses spécificités, ses particularités. C'est pourquoi l'essence d'une guerre dans laquelle la Russie ou ses alliés risqueraient d'être entraînés est très difficilement prédictible. Cependant, cette capacité de prévision nous est indispensable. Car dans les sciences militaires, toute position théorique non prédictive est sans valeur[1]. »

Réguler le cybermonde c'est donc d'abord associer, en des équipes dédiées, des capacités d'imagination, d'anticipation, des facultés à diagnostiquer juste et à temps. Le tout visant à concevoir des stratégies, sans doute pertinentes, mais aussi prudentes, s'agissant d'un univers numérique plutôt fragile. Cela s'appelle le décèlement précoce. Quand est assuré ce savoir qui pressent, quand il est mis au service de la société, tout le high-tech devient infiniment précieux.

1. *Courrier Militaro-Industriel*, Moscou, « The value of science in prediction »

# Conclusion

## L'AVENIR RADIEUX DU CYBERCRIME ?

Comment conclure l'étude d'un phénomène aussi planétaire, exponentiel et cataclysmique ? D'abord en laissant venir vers nous ce qui apparaît, afin de pouvoir scruter sans qu'il nous engloutisse ce que Martin Heidegger nommait « l'abîme incréé où tremble et est contenu tout ce qui se prépare à survenir ».

« Tout ce qui se prépare à survenir » dans le cybermonde nous est-il accessible ? Commence-t-on à y entrevoir son magma menaçant ? Pour répondre, il suffit d'aller à la bonne source et d'y observer ce qui, dans son sens original, en résulte. En l'occurrence, la bonne source est la Black Hat * Convention, organisée chaque été à Las Vegas dont la vocation est d'alerter et d'échanger sur les menaces numériques émergentes. Dans cette enceinte, diverses catégories de geeks viennent fièrement y annoncer comment ils ont infiltré tel serveur ou réseau, cassé tel code ou contrôlé tel logiciel. Examinons donc ce qu'en ce mois d'août 2014, les vigies de Black Hat signalaient comme dangers à l'horizon.

- domotique : prendre en quelques instants le contrôle de toutes les chambres d'un hôtel, chauffage, lumières, stores et rideaux, tout ce qu'on peut y régler à l'aide d'un ordinateur.
- ventes en ligne : pirater les points de vente mobiles (*mobile points of sale*, MPOS) grâce à des cartes de paiement toxiques, à l'aide desquelles on infiltre un maliciel dans un serveur MPOS.
- sécurité d'un ordinateur ou d'une tablette : décrypter les mots de passe tapés par un usager à l'aide de la caméra des Google Glasses

et à plus de trois mètres.

- sécurité du cloud : pirater Amazon web Services, AWS (le cloud d'Amazon) et y siphonner les données, y créer des contacts et identités factices en vue de diverses fraudes.
- aéronautique : pirater les systèmes de communication par satellite (SATCOM) utilisées par les navires, les avions, les forces armées, les services d'urgence, les plateformes pétrolières, les réseaux de pipelines, etc. Les dispositifs SATCOM comporteraient des failles. En passant par les systèmes Wi-Fi ou de vidéo des passagers à bord, le pirate peut ensuite « piéger » l'avionique de l'aéronef et ainsi interférer avec sa navigation.
- réseaux sociaux : siphonner les informations de 100 millions d'usagers en une semaine avec un investissement initial de 150 dollars.
- bus informatique USB (Universal Serial Bus, bus universel de série) : sont visées les clés USB pour stocker et transmettre des fichiers mais aussi les claviers, les souris et les dispositifs de rechargement de batterie qui utilisent la norme USB. Celle-ci est piratable car les micrologiciels (pilotes, drivers, etc.) qu'elle utilise pour fonctionner sont inscrits sur des puces et non téléchargés sur un disque dur d'ordinateur. Or les logiciels antivirus ne bloquent que les maliciels copiés sur la mémoire de l'ordinateur et non ceux des pilotes ou drivers qu'ils ne détectent pas. Une fois infiltrés par USB, ces maliciels affectent non seulement les ordinateurs, mais aussi l'électronique de grande consommation, voire celle d'infrastructures critiques.

Allons plus loin : partout et toujours, les criminels de carrière sont des prédateurs et ne sont que cela. Ils maîtrisent quelques pratiques simples, efficaces et brutales, leur permettant de flairer les occasions lucratives, puis de séduire, corrompre, intimider, tuer ou réduire en esclavage ceux dont l'exploitation leur permet de gagner rapidement le plus d'argent possible. Comment, à l'horizon 2020, les criminels, terroristes ou hybrides perturberont ou pilleront le cybermonde, voilà sur quoi nous allons ouvrir quelques perspectives.

# L'économie de l'information risque de coûter cher

D’ici 2020, la cybercriminalité risque de faire perdre 3 000 milliards de dollars à l’économie mondiale. On obtient ce total en prenant en compte des attaques plus graves et fréquentes de pirates toujours plus experts, des gouvernements ajoutant au désastre par leur dirigisme et leurs maladresses, des usagers victimes de la foire d’empoigne dans les technologies mobiles et le cloud computing.

## Big (Cyber) Brother se régale

Alors que les honnêtes gens du cybermonde glosent sur l’utilité ou les risques d’une cyber-identité universelle et à vie, sur l’effet qu’aurait une telle mesure sur le cybercrime, on apprend qu’à l’été 2013, une société privée de marketing (Renew London) a installé dans les poubelles publiques de la capitale britannique des systèmes de capteurs électroniques qui, sans aucune autorisation, récoltent des masses de données provenant des téléphones portables des passants. Scandale, excuses et fin de l’opération. Mais pour un cyber-flicage de ce type repéré, combien d’autres, actifs et invisibles ? Un autre dispositif de *crowd scanning*, le BOSS (Biometric Optical Surveillance System) associe ordinateurs et caméras, et identifie automatiquement les visages des passants dans les rues (jusqu’à 100 m) avant de les comparer à des *watch lists* avec une efficacité de 80 à 90 %.

Mais, comme on l’a vu plus haut, les *watch lists* américaines ne sont pas au point. À cause d’elles, le sénateur Edward Kennedy fut naguère débarqué d’un avion parce qu’on l’avait confondu avec un homonyme de l’IRA et les terroristes tchétchènes de Boston, pourtant maintes fois signalés par Moscou, furent totalement négligés jusqu’à ce qu’ils commettent leur attentat.

## Massification des offensives

En 2013, les déjà classiques attaques par déni de service (DDoS) ont été plus intenses, vigoureuses, plus rapides et difficiles à contrer. Selon le *Worldwide Infrastructure Security Report*, une attaque en 2013 a atteint les 309 gigabits par seconde (Gbps), contre 100 Gbps en moyenne pour les plus fortes de 2010 à 2012. Une tendance à la massification offensive qui devrait perdurer ces prochaines années.

# L’Internet (criminel) des objets

La connectivité des objets avec l’homme et entre eux est destinée à conduire toute activité humaine. Selon Shodan (le Google des objets connectés) tout sera, ou est déjà, connecté à Internet. Les réseaux d’eau et d’électricité, les bâtiments, les usines, la circulation routière, les feux de circulation, les caméras de sécurité CCTV, les éoliennes, les barrages et même les accélérateurs de particules. Cisco et IBM annoncent 50 milliards de machines connectées en 2020. La planète comptera bientôt plus d’objets connectés à d’autres objets que d’humains connectés entre eux. Mais, selon les experts, ces systèmes connectés sont en majorité mal sécurisés, donc piratables. Tel est le champ de bataille des cyber-pirates d’aujourd’hui, des systèmes high-tech des véhicules et des réseaux à ceux implantés dans le corps humain et des domiciles.

Dans la maison connectée, un téléphone mobile ou une tablette peuvent tout contrôler : verrous, lumière, électroménager. Sans parler de la brosse à dents qui prend les rendez-vous chez le dentiste ; le frigidaire qui passe seul ses propres commandes ou du réveil qui met en marche lui-même la cafetière. Dans cet environnement, tout est évidemment possible si la sécurisation du dispositif n’est pas optimale, et sans cesse remise à niveau. Faute de quoi, ces objets risquent d’être contrôlés à distance par des pirates, ou encore verrouillés contre rançon comme c’est arrivé en mars 2014, en Australie, quand un pirate a pu bloquer les ordinateurs, tablettes et smartphones d’une maison et exiger 100 dollars par appareil pour les « libérer ».

Hors de chez lui maintenant, chaque individu risque de vivre un cauchemar numérique quotidien, un *1984* en pire. En termes d’intrusions publicitaires non sollicitées, l’Internet des objets est un cauchemar digital (rappel : dans les États de droit, le harcèlement publicitaire est une infraction, punie par la loi). Sans cesse espionné par son environnement familier – l’écran de sa voiture, sa montre, ses lunettes, sa brosse à dents, son frigidaire, les thermostats de son domicile, tous devenus « intelligents », car connectés à un ordinateur ou un smartphone – tout individu connecté sera bombardé de publicités. Google s’y prépare.

Quant aux voitures, elles pourront se passer de conducteur. En septembre 2013, Alan Mulally, P-DG de Ford, l’a annoncé ainsi : « La voiture devient un terminal Internet comme un smartphone ». Un objet

connecté de plus, dans la mesure où il contient de 10 à 40 micro-ordinateurs, qui devient donc aussi piratable qu'un ordinateur. Et toujours plus de véhicules sont connectés à Internet : 45 millions l'étaient en 2013, 420 millions le seront probablement en 2018. Sans oublier les véhicules utilitaires. À l'été 2014, Daimler présente le camion du futur, à bord duquel le pilote suit la conduite sur une tablette, les bras croisés, tel le commandant de bord d'un avion sous pilotage automatique. Le chauffeur fait démarrer l'engin, l'insère dans la circulation et quand il atteint les 80 km/h, enclenche le pilote automatique. Dès lors, des capteurs scrutent les 70 à 250 m autour du camion, tandis que l'ordinateur de bord distingue les routes à une et deux voies, reconnaît les piétons et les objets fixes ou mobiles, puis réagit en conséquence.

Dès aujourd'hui et grâce à Internet, un véhicule peut se gérer à distance : ouverture des serrures, contrôle des phares, de l'autoradio, des essuie-glaces et du compteur, écrans multimédias, commandes vocales, aide au stationnement, assistance en ligne… Vers 2020, les véhicules se conduiront vraiment tout seuls, grâce à des systèmes de pilotage autonomes et autres « chauffeurs électroniques ». Mais les risques sont à la mesure de ces avancées technologiques. Peu chers, aisément accessibles en ligne, de multiples outils illégaux ont renouvelé la panoplie du voleur de véhicules : clés électroniques programmables, émetteurs sans fil permettant l'ouverture des portières, boîtiers ou cartes informatiques permettant de pirater le système antipiratage du véhicule. Et arrivera bientôt sur le marché un boîtier sans fil, bon marché et plus petit qu'un smartphone, permettant sans contact physique, de se connecter à l'électronique de bord de tout véhicule.

Or, sur tous les véhicules connectés, se connecter à la prise OBD (On Board Diagnosis) permet de désactiver l'antivol, voire de contrôler un véhicule qui roule : sa voiture accélère ou freine, son volant tourne, ses phares s'éteignent et le conducteur est impuissant. Ces risques sont bien réels et pourraient revêtir une dimension criminelle ou terroriste difficilement parable.

# Des Botnets hors de tout contrôle

Sur les réseaux sociaux, on a vu qu'il est désormais possible de se créer un public factice d'amis fidèles, multipliant à votre propos les commentaires positifs. On vous les vend désormais en gros ou au détail sur

des sites spécialisés appelés *Bots Farms*. Programmés pour imiter le comportement humain, ces « amis » ont désormais des noms plausibles, des horaires d'humains vrais, des activités réalistes et dialoguent même entre eux. D'ores et déjà, on compte des millions de ces « amis » fictifs sur Internet. Or de par leur masse même, ces citoyens imaginaires du cybermonde influencent désormais la cyber-opinion publique. Aux États-Unis, certains estiment que les agences de marketing politique en font un usage important. Aujourd'hui, Google, Facebook et Twitter sont obligés d'engager des *Bots Hunters* pour éliminer ces « faux amis ».

Là où la réalité commence à dépasser la fiction, des Bots parviennent à parfaitement imiter des téléphones portables, recevant de *faux* signaux GPS, requis par de *faux* humains et conduisant de *fausses* voitures. Résultat d'une récente expérience : Waze, le site et logiciel de géolocalisation de Google, a « vu » des embouteillages dans certaines parties de Tel Aviv et en a détourné les (vrais) conducteurs de (vraies) automobiles. Alors qu'il n'y avait pas le moindre bouchon là ou Waze le « voyait », mais un simple piratage commis par des étudiants[1].

C'est donc principalement à la *nature* même de la réalité qui s'effiloche chaque jour un peu plus sous les coups du virtuel, qu'il faudra être attentif. Là se trouvent les grands champs de bataille de la cyber-sécurité. Car chaque jour, la marée cybercriminelle monte un peu plus haut. Au moment d'achever ce livre, on apprend ainsi que d'obscurs pirates, peut-être russes, installés « quelque part entre le Kazakhstan et la Mongolie », ont pénétré 420 000 sites Internet, des plus petits aux plus grands, en utilisant la technique de « l'injection SQL » (pour *Structured Query Language*, langage structuré de requête) qui permet de piller des bases de données sans être repéré.

Partant de 500 millions de comptes-courriels ainsi fracturés, ils y ont siphonné le chiffre vertigineux d'un milliard deux cent millions de données sensibles, mots de passes, noms d'utilisateurs, codes d'accès, etc. Pour le *New York Times,* « dans la sécurité informatique, certains craignent que tenir les informations personnelles hors de portée des bandits soit une bataille quasiment perdue ».

Des experts s'alarment déjà de l'apparition, sans doute postérieure à l'horizon 2020, des ordinateurs quantiques capables d'effectuer chaque seconde des milliers de milliards de calculs. D'ici la mise en service du plus basique de ces ordinateurs, toute la pratique du cryptage est à revoir de fond

en comble. Pour des ordinateurs aussi puissants et ultrarapides, casser les codes actuels les plus complexes sera un jeu d'enfant. Un problème de taille puisque, au fond, le cybermonde tout entier n'est qu'un château de cartes reposant sur un socle : le codage de tout ce qu'il contient de sensible. Le plus banal des appels de téléphone mobile, le plus simple des virements dépendent d'un système codé, sans l'étanchéité duquel tout le système, puis tout l'Internet, s'effondre. Serons-nous prêts à temps ? Rien aujourd'hui ne l'assure.

Ces batailles pour sécuriser l'Internet, il y en aura évidemment d'autres mais, pour la plupart, y compris dans le domaine de « l'inconnu-inconnu », les principes et méthodes exposés dans ces pages, la pratique du décèlement précoce des dangers et menaces, devraient permettre d'éviter les surprises dramatiques et autres chocs stratégiques. Et d'agir à temps.

1. *Popular Science*, 31/03/2014, « Israeli Students Spoof Waze App With Fake Traffic Jam – The future of cyber attacks is mildly annoying ».

# ANNEXES

# Annexe I

# *LE CHAMP PRÉALABLE D'INSPECTION*

Trop souvent, la société de l'information néglige le contexte dans lequel, pour un criminologue par exemple, un crime est commis. Or tout phénomène s'inscrit dans un « champ préalable d'inspection » et le considérer est essentiel, car il détermine toute compréhension ultérieure. Sans la prise en compte de ce champ, nulle action n'est durablement efficace. Il faut donc commencer par observer le champ préalable d'inspection de tout phénomène dangereux.

Mais quel est ce champ ? Une image peut le décrire : seul le fait d'avoir d'abord compris ce qu'est le *temps* permet ensuite de réaliser quel est l'usage d'une montre. La notion de temps est le « champ préalable d'inspection » expliquant l'usage de la montre. Il en va ainsi pour tout phénomène : « Toute investigation nécessite un monde déjà ouvert à l'intérieur duquel son mouvement devient possible. Or c'est précisément dans l'ouverture d'un tel secteur d'investigation que consiste le processus fondamental de la recherche[1] ».

Pour ce qui nous occupe ici, le champ préalable d'inspection est l'approche attentive de la réalité criminelle afin d'en éliminer tous les préjugés, illusions, vieilleries, fantasmes et phobies constituant les scories (« évidences courantes », « pensée unique ») de la société de l'information.

Voici comment un militaire révèle l'utilité cruciale de cette pratique, en matière stratégique : « Dans une ère d'affrontements asymétriques, il importe d'acquérir une intelligence approfondie des éléments non-militaires, pour comprendre la vie dans l'autre camp. Les services spéciaux doivent pouvoir pénétrer les couches superficielles de cet autre camp, et

accéder à son cœur. Ils doivent goûter la poésie du camp d'en face et pratiquer sa culture[2] ».

1. Martin Heidegger, *Chemins qui ne mènent nulle part – Le temps des conceptions du monde*, NRF-Gallimard.

2. « A critical look at intelligence », Aharon Ze'evi, chef du renseignement militaire israélien, 2002-2006. *Strategic Assessment*, Israël, mars 2007.

# Annexe II

# *SINGULARITY* (SINGULARITÉ TECHNOLOGIQUE)

La notion de « singularité » apparaît à la fin de la décennie 1950, lors d'échanges savants entre mathématiciens et physiciens. Voici un extrait de l'article du mathématicien Stanislaw Ulam, évoquant ses entretiens avec un autre mathématicien et physicien éminent, John von Neumann : « Notre conversation s'est focalisée sur l'incessante accélération de la technologie et sur les changements de l'existence humaine, qui semble approcher une *singularité* [nous soulignons] essentielle pour l'histoire de notre espèce ; seuil au-delà duquel la conduite des affaires humaines, telles qu'elles existent à présent, ne saurait perdurer[1] ».

En 1993, l'écrivain de science-fiction américain Vernor Vinge invente le terme de « singularité technologique[2] » et en 2010 le chercheur, vulgarisateur et écrivain suédois Anders Sandberg tente de maintenir le concept de singularité au niveau sérieux de la recherche scientifique, lors de la conférence « The future of Artificial general Intelligence workshop, Lugano, march 2010 ». L'intervention de Sandberg s'intitule : « An overview of models of technological singularity ».

Mais déjà, une autre acception de la « Singularité » a commencé à s'imposer dans les médias et dans l'opinion, peu scientifique mais plutôt de type pensée magique, ou croyance sectaire. Pour le futuriste assez fantaisiste Ray Kurzweil, Internet deviendra un jour une sorte de super-cerveau, de super-intelligence connectée-unifiée, surplombant et conduisant, à l'instar d'un dieu, l'humanité tout entière. D'où la prudente approche du chercheur britannique Nick Bostrom dont l'ouvrage

*Superintelligence – paths, dangers, strategies* (Oxford University Press, Oxford UK, 2014) fait autorité : « Le terme de singularité… a été utilisé dans la confusion, pour produire nombre d'acceptions disparates ; il a fini par susciter une malsaine et quasi-millénariste ambiance de type techno-futuriste ». Autrement dit, c'est une forme de science-fiction pour naïfs.

1. *Bulletin of the American Mathematical Society,* 1958, Stanislaw Ulam – John von Neumann.

2. NASA Lewis research Center, NASA Conference Publication 10129, « Vision 21: interdisciplinary science and engineering in the era of cyberspace » – Vernor Vinge : « The coming technological singularity – how to survive in the post-human era »

# Annexe III

# *L'APPAREIL DE CYBER-SÉCURITÉ DES ÉTATS-UNIS*

Le « US Military Cyber Command » a été créé en 2010. Son domaine opérationnel est le cyberespace. Il réunit tous les militaires américains impliqués dans le *cyber* : Army Ninth Signal Command, Navy Tenth Fleet (cybercommand), etc., soit plus de 60 000 personnels.

Sa mission est la suivante : « US CYBERCOM planifie, coordonne, intègre, synchronise et conduit les opérations et actions de défense des réseaux d'information spécifiques du ministère de la Défense. Il s'entraîne à – et s'il en reçoit l'ordre, mène – des opérations militaires de tout type dans le cyberespace dans le but d'assurer la liberté des États-Unis et de leurs alliés dans cet espace, tout en la déniant à nos adversaires ».

En tant qu'état-major, CYBERCOM disposait fin 2012 d'environ 900 hommes, destinés à atteindre 5 000 personnes en quelques années. Son siège est implanté à Fort Meade (Maryland) face à celui de la NSA. En 2014, le budget de CYBERCOM a doublé, alors que tous les autres budgets militaires baissent. Pour les cinq années à venir, le Pentagone a prévu un budget de 23 milliards de dollars pour la cyber-défense, qu'il tente de faire approuver par le Sénat.

Les trois missions de CYBERCOM sont les *National Mission Force* dédiée à la protection des infrastructures informatique américaines (électricité, téléphone, etc.) ; *Combat Mission Force* pour les opérations offensives ; *Cyberprotection Force* pour la protection des ordinateurs et réseaux du Pentagone et plus largement, militaires.

Par ailleurs, le Department of Homeland Security dispose d'une National Cyber Security Division qui supervise notamment l'United States Computer Emergency Response Team (US-CERT*), tour de contrôle d'expertise technique, de collaboration public privé et de dissémination d'informations sur la sécurité informatique.

# Annexe IV

# *LES EUROPÉENS ET LA CYBER-SÉCURITÉ*

Selon le Special Eurobarometer/390 *Cyber security Report* de juillet 2012 (sondage auprès des citoyens des 27 pays alors de l'Union européenne), sur 100 Européens :

53 % vont sur Internet au minimum une fois par jour

13 % une fois par semaine

3 % une fois par mois

2 % moins encore.

29 % ne vont jamais sur Internet

53 % achètent des biens et services sur Internet

52 % fréquentent des réseaux sociaux

48 % usent d'une banque en ligne

Dans la tranche d'âge des 15-24 ans, 84 % vont sur Internet au minimum une fois par jour et 4 % ne vont jamais sur Internet.

74 % des internautes de l'UE estiment courir plus de risques qu'en 2011 ; 61 % ont peur du vol d'identité.

Quand ils effectuent des achats sur Internet, ou font des transactions bancaires en ligne, les soucis majeurs des Européens sont :

– Le vol de données personnelles (40 % de ceux qui usent de banques en ligne)

– La sécurité des paiements en ligne (38 % de ceux qui achètent sur Internet)

– Ne pas recevoir sa commande en ligne (19 % de ceux qui achètent sur Internet)

– N’ont pas de souci : 21 % de ceux qui achètent sur Internet.

Sur les risques du cybercrime, 59 % des internautes européens s’estiment mal ou pas informés sur ce point et 38 % s’estiment assez ou bien informés.

Parmi les internautes de l’EU, 12 % ont déjà été victimes de fraudes (en général) en ligne et 8 % de fraudes *identitaires* en ligne. En novembre 2013, 76 % des résidents de l’UE estimaient que le risque d’être victimes du cybercrime a augmenté depuis un an.

# DIRECTIVES ET TEXTES EUROPÉENS SUR LA CYBERSÉCURITÉ

La *Directive 2013/40/EU* sur les attaques visant les systèmes d’information est destinée à harmoniser les législations pénales en la matière. Elle porte sur :

– les accès illégaux et intrusions dans les systèmes d’information,

– les interférences illégales et interceptions visant les systèmes et les données,

– la facilitation de la coopération entre services officiels concernés des États-membres.

La stratégie de cybersécurité adoptée en février 2013 vise à faire de l’UE l’environnement en ligne le plus sûr au monde pour Internet. La même année, une tour de contrôle européenne pour le cybercrime est créée à Europol (La Haye, Pays-Bas), sous le nom d’EC3 Center.

# Annexe V

# *LES CRYPTO-MONNAIES (CM) ALTERNATIVES AU BITCOIN*

En anglais, le nom générique de ces crypto-monnaies est altcoin, ou *alternate cryptocurrencies*. Il en existait environ 140, début 2014, de divers types :

– Altcoins utilisant le même algorithme de cryptage que bitcoin (SHA256) : namecoin (NMC), peercoin (PPC), devcoin (DVC), terracoin (TRC), etc. ; une quinzaine en tout.

– Altcoins utilisant un algorithme Scrypt (cryptage très lourd et difficile à casser) : litecoin (LTC), novacoin (NVC), feathercoin (FTC), worldcoin (WDC), etc. ; une quinzaine en tout.

– Crypto-monnaies alternatives utilisant des algorithmes originaux : ripple (XRP) primecoin (XPM), quark (QRC), securecoin (SRC) et même – Ô mânes de Lovecraft ! – un délicieux offeringstocthulhu (OFF) ; une quinzaine en tout.

Toutes ces cyber-devises, ont en commun :

– d'avoir un volume d'émission limité et contrôlé,

– d'être créées loin de tout gouvernement par pure voie électronique-informatique, cryptées et échangées entre des usagers qui les conservent dans des cyber-portefeuilles,

– d'être anonymes, décentralisées et intraçables : impossible ici de lier une transaction à un individu, de remonter à qui a acheté ou vendu quoi que ce soit dans une bourse d'échange en ligne, ou converti une somme d'une altcoin en devises ou l'inverse,

– de fonctionner en mode peer-to-peer-networks, avec transmission mondiale ultrarapide, de dix minutes à une heure, confirmations et vérifications incluses,

– d'être très spéculatives avec des taux de changes erratiques (la volatilité de bitcoin est de 20 à 30 % par jour)

– de permettre d'acheter des biens et services dans le monde réel et d'être échangeables contre des monnaies nationales réelles (monnaies digitales), contrairement aux monnaies virtuelles (réservées au seul cybermonde, jeux en ligne, etc.). Grâce à une clé privée, le payeur contrôle son versement jusqu'à l'issue mutuellement acceptée de la transaction.

– d'être très difficiles à réguler, taxer ou confisquer par des États.

Au printemps 2014, leur volume total en euros était de 7,3 milliards d'euros, dont 5,6 milliards pour le seul bitcoin. Soit, au total, 0,8 % de la masse monétaire mondiale (MMM), chiffre qui atteindra probablement 1,7 % de la MMM en 2015. Au même moment, les trois crypto-monnaies majeures (bitcoin, ripple, litecoin) représentaient les 90 % de toutes les crypto-monnaies.

De 2012 à 2014, l'usage des crypto-monnaies explose : de janvier à avril 2013, on a constaté 1 789 % d'augmentation.

# RÉFÉRENCES,
# SOURCES & CITATIONS

– Provenant des médias (articles, enquêtes, etc.), de journaux, revues, magazines, sites d'information, etc., ci-après indiqués M,

– Provenant d'ouvrages de tous types, ci-après indiqués L,

– Provenant de rapports officiels, ou d'organisations internationales, ci-après indiqués D,

Toutes ces sources sont classées par mention dans chaque partie et chapitre du livre ; à l'intérieur de ceux-ci, par ordre d'évocation dans le texte.

## GLOSSAIRE

D – US Army War College, 2009, Strategy research Project, « Defining and deterring cyberwar »

M – *Bloomberg – Business Week*, 20/07/2011, « Cyberweapons: the new arms race »

M – *New York Times*, 11/08/2014, « How working from home can leave an opening for hackers »

M – *Le Monde*, 11/06/2014, « Le hasard, arme contre les pirates numériques »

M – *New York Times*, 2/01/2014, « The Snowden effect: 2 pioneers debate the future of the net »

M – *Nouvel Observateur*, 6/08/2014, « 1,2 milliard de données piratées : une attaque simple et structurée »

# PRÉAMBULE

M – *New York Times*, 11/08/2014, « The promise of new cities where data builds roads »

M – *Agence France Presse*, 2 mai 2014, « Dozens held in Philippines over global “sextortion” ring »

L – Les indispensables œuvres de Philip K. Dick, de préférence en anglais ; consulter par exemple <goodreads.com/author/show/4764.Philip_K_Dick>

M – *International Herald Tribune*, 23/08/2013, « Cutting power to all those screens: advice in 3 volumes »

M – *BBC News*, 31/07/2014, « Avoid data breaches and keep the cyberthieves at bay »

M – *The Economist*, 26/07/2014, « Virtual depravity »

L – Martin Heidegger, *Apports à la philosophie – De l’avenance*, NRF-Gallimard, 2013

M – *Revue de la Gendarmerie nationale*, 4e trimestre 2012, « Quelles menaces majeures pour les utilisateurs de réseaux numériques dans un futur proche ? »

D – SGDSN, décembre 2012, « Contribution de l’ANSSI au futur Livre Blanc sur la Défense et la Sécurité Intérieure »

L – Jaron Lanier, *Who Owns The Future ?*, Simon & Schuster NY, 2013

L – PW Singer, Allan Friedman, *Cybersecurity and cyberwar – what everyone needs to know*, Oxford University Press, NY, 2014

L – Eric Schmidt, Jared Cohen, *The new digital age – reshaping the future of people, nations and business*, John Murray London UK, 2013

M – *New York Review Of Books*, 14/08/2014, « The hi-tech mess of higher education »

M – *Huffington Post*, 25/07/2014, « 70 % of child sex trafficking victims are sold online: study »

# PARTIE 1 – CHAMP DE BATAILLE ET CADRE LARGE

L – Raymond Ruyer, *La Gnose de Princeton*, Fayard, 1974

M – *Le Monde* – Internet Activ', 16/05/2014, « Le problème de la gauche avec Internet »

M – *Le Monde*, 22/08/2014, « Combien coûterait Internet sans publicité ? »

D – Massachusetts Institute of Technology, Cambridge, Ma., Juillet 1992, David Clark, « A cloudy crystal ball – visions of the future »

M – *Le Monde* – Sciences et Techno, 18/04/2013, « Google et les Transhumanistes »

M – *Le Point*, 29/03/2014, « Singularity University, escale dans le futur »

M – *Nouvel Observateur*, 13/04/2014, « Micro-États, villes flottantes : le projet fou des nouveaux maîtres du monde »

L – Ray Kurzweil, *The age of spiritual machines, when computers exceed human intelligence*, Viking, NY, 1999

L – Frédéric Gros, *Le Principe sécurité*, NRF-Gallimard, 2012

M – *Challenges*, 1/07/2014, « La révolution numérique va-t-elle tuer le capitalisme ? »

M – *USA Today*, 2/07/2014, « In the year 2025, the world will be a much smaller place »

M – *Policy Horizons Canada*, 4/06/2014, « Emerging neurotechnologies that will change the world »

M – *New York Times International*, 11/06/2014, « Intelligence too big for a single machine »

M – *Mashable*, 3/08/2014, « Elon Musk says artificial intelligence could be more dangerous than nukes »

M – *New York Times International*, 11/04/2014, « Brokers fight to manage Tech Stars new wealth »

M – *Le Monde*, 5/02/2014, « Yahoo ! France passe sous droit irlandais »

M – *Les Echos*, 23/08/2013, « Aux États-Unis, Yahoo ! rivalise de nouveau avec Google »

M – *New York Times International*, 4/08/2014, « Facebook's gateway drug »

M – *New York Times International*, 7/08/2014, « Tech giants turning into conglomerates »

M – *Le Figaro*, 17/09/2013, « Les millionnaires du net investissent dans la Silicon Valley »

M – *New York Times International*, 6/11/2013, « Bezos and the one-click wonder »

M – *Le Monde-Magazine*, 14/09/13, « La méthode Jeff Bezos »

M – *Wired*, 25/07/2014, « Amazon's cloud is growing so fast it's scaring shareholders »

M – *GeekWire*, 25/07/2014, « Chart: Amazon now employs 132 000, more than tripling in the past three years »

M – *New York Review Of Books*, 10/07/2014, « Citizen Bezos »

M – *New York Times International*, 14/04/2014, « Oracle's chief makes no apologies for lofty pay »

M – *New York Times International*, 20/04/2014, « Silicon Valley's big paydays get a pass »

M – *International Herald Tribune*, 13/08/2013, « Digital tycoons lend a hand to the print media battered by their success »

M – *International Herald Tribune*, 10/08/2013, « For journalistic greatness, the old model seems all but dead »

M – *Daily Telegraph*, 16/04/2014, « The US is an oligarchy, study concludes »

M – *New York Times International*, 21/04/2014, « Paying the price for security without cost »

M – *Bloomberg-Newsweek*, 5/05/2014, « Tech Hubris »

M – *L'Expansion,* 30/06/2014, « Oui, Facebook nous a manipulés (et ce n'est pas près de s'arrêter) »

M – *International Herald Tribune*, 23/08/2013, « Struggling to adapt, technology titan's earnings show strain »

M – *Le Figaro*, 6/09/2013, « Pixmania, la chute éclair d'une étoile du web »

# PARTIE 2 – LES CHAMPS DU CYBERCRIMINOGÈNE

D – OCDE – TF-CIT, 5-7/03/2014, « Illicit financial flows – methodologies for measurement and the use of virtual currencies as a money-laundering tool »

M – Altcoins, voir le site <altcoins.com>

M – *Business Insider*, 3/12/2013, « Why bitcoin and other cryptocurrencies will inevitably become tools of the rich, powerful and criminal »

M – site *Dark Reading*, 18/02/2014, « Bye bitcoin, criminals seek other cryptocurrency »

M – *Le Monde*, 30/05/2013, « L'affaire Liberty Reserve révèle les liens entre monnaies virtuelles et criminalité »

M – *Le Monde*, 28/05/2014, « Monnaies électroniques, la mode du Dark »

M – *Wall Street Journal*, 7/04/2014, « Bitcoin's boosters struggle to shore up confidence »

M – *Le Monde*, 15/05/2014, « Mt.Gox : retour sur les ratés du bitcoin »

M – *Journal du Dimanche*, 1/06/2014, « Le bitcoin ouvre sa première "banque" »

M – *Nouvel Observateur*, 25/02/2014, « bitcoin : crise réelle pour monnaie virtuelle »

M – *Le Monde*, 27/02/2014, « La monnaie virtuelle bitcoin vit son premier krach »

M – *New York Times*, 4/03/2013, « bitcoin heist exposes a regulatory puzzle »

M – *Agence France-Presse*, 9/03/2014, « Mt.Gox faced 150 000 attacks per second »

M – *Agence France-Presse*, 26/03/2014, « Mt.Gox collabore avec la police japonaise »

M – *Le Parisien*, 4/03/2014, « bitcoin : encore une plateforme braquée par des pirates »

M – *Associated Press*, 5/03/2014, « bitcoin : une autre plateforme ferme ses portes »

M – *Le Parisien*, 6/03/2014, « bitcoin : mort “non naturelle” de la jeune dirigeante de First Meta »

M – *Le Monde*, 27/01/2014, « L’opérateur d’une bourse d’échange de bitcoins arrêté pour blanchiment »

M – site *Chicago Syndicate*, 27/01/2014, « DEA charges bitcoin exchange companies for laundering Silkroad drug money »

M – site *International Business Crime*, 15/04/2014, « Cryptocurrency new round up »

M – *New York Times International*, 26/02/2014, « Troubled exchange tests bitcoin faithful »

M – *Le Figaro*, 22/04/14, « Des distributeurs de bitcoins voient le jour partout dans le monde »

M – *Le Figaro*, 26/05/14, « Des distributeurs de bitcoins à Las Vegas et à Paris »

M – *Le Figaro*, 11/04/14, « La folie bitcoin de la Silicon Valley »

M – *Reuters*, 9/05/2014, « Aux États-Unis, le bitcoin pourra financer les campagnes politiques »

M – *Techcrunch*, 13/06/2014, « Boom goes the bitcoin »

M – *Libération*, 17/07/2014, « Vers une régulation du bitcoin »

M – *Business Insider*, 21/07/2014, « Why bitcoin is “good money” for the digital era »

M – *Le Monde*, 7/07/2014, « Un trafic de bitcoins démantelé en France »

M – *New York Times International*, 30/06/2014, « US auctions bitcoin trove seized in raid »

M – *Daily Telegraph*, 21/07/2014, « Dell jumps on the bitcoin bandwagon »

M – *Les Echos*, 7/02/2014, « La “datafication” du monde »

M – *Le Monde*, 18/04/2014, « Big Data vous regarde »

M – site *PC*, 26/03/2014, « Big Data is just a big scam »

M – *New York Times International*, 10/04/2014, « IBM bets Watson can earn its keeps »

M – *Le Figaro*, 2/04/14, « Le marché Big Data, nouveau graal de l'informatique »

M – *Nouvel Observateur*, 21/04/2014, « Pourquoi la Big Data devient un très gros business »

M – *Le Monde*, 8/05/2014, « Enseignement supérieur : la mine d'or du Big Data »

M – *New York Review Of Books*, 7/11/2013, « Are we puppets in a wired world ? »

M – *New York Times,* 16/06/12, « Acxiom, the quiet giant of consumer database marketing »

M – *Financial Times*, 23/07/2014, « Google catches cold as debate over "big data hubris" rages »

M – *Le Figaro*, 7/07/2014, « Big Data : le plan de la France pour concurrencer les géants américains »

M – *Mediapart*, 14/04/14, « Le trading de haute fréquence est un système de fraude de grande ampleur »

M – *New York Times International*, 04/2014, « Stepping up the scrutiny of Wall Street's warp-speed ways »

M – *New York Times International*, 2/04/2014, « Fault runs deep in fast trading »

M – *New York Times International*, 2/04/2014, « Heroes trying to hobble Wall Street cowboys »

M – *New York Times International*, 1/04/2014 – « Writer decries a "rigged" stock market »

M – *New York Review Of Books*, 10/07/2014, « High on speed »

M – *CNN*, 13/08/2014, « The high-tech arm's race that's causing stock market tsunamis »

M – *Les Echos*, 23/06/2014, « Un trader haute fréquence victime d'une cyberattaque très sophistiquée »

M – *Paris Match*, 24/07/2014, « Chris Dancy, l'homme le plus connecté du monde »

M – *Daily Mail*, 17/07/2014, « Picture purr-fect! Smart cat feeder uses facial recognition technology to monitor how much your cat eats – and tells

you if they're greedy »

M – *Daily Telegraph*, 21/07/2014, « Worried your partner might be having an affair ? There is an app. for that »

M – *New York Times International*, 21/07/2014, « Algorithms to help pick roommates »

# PARTIE 3 – MÉANDRES ET PERCÉE DU CYBERCRIME

M – site *Facts Hunt*, <www.factshunt.com>

M – *New York Times International*, 21/08/2014, « Recording the scene of every crime »

M – *Le Figaro*, 22/04/2014, « Faut-il avoir peur de Big data ? »

D – ITU-ICT – Facts and Figures, « The world in 2014 »

D – *Report* – McAfee & CSIS, July 2013, « The economic impact of cybercrime and cyber espionage »

M – *Bloomberg*, 9/06/2014, « Cybercrime remains growth industry with $ 445 billion cost »

M – site *ZD Net*, 4/04/2014, « Cybercriminals are outspending the defenders two to one: HP »

M – *Daily Mail*, 12/08/2014, « Half of us are at risk of cyber-attacks because we don't install antivirus software on laptops and phones »

M – site *HighTech Bridge*, 18/02/2014, « 300 000 compromised accounts available on Pastebin: just the tip of cybercrime iceberg »

M – *News 24*, 26/04/13, « Organised crime linked to IP theft »

M – *The Inquirer*, 25/04/2013, « FBI says cybercrime is emerging as a threat to surpass terrorism »

M – *Le Figaro*, 19/11/2013, « L'État et les entreprises face aux cybermenaces »

M – *Evening Standard*, 28/04/2014, « Seven out of ten frauds are now cybercrimes, police chief warns »

M – *Pro Publica*, 12/06/2014, « Why online tracking is getting creepier »

M – *Le Monde*, 24/08/2013, « Une panne informatique sur le Nasdaq révèle la vulnérabilité des Bourses »

M – *Le Figaro*, 26/08/12, « Série noire informatique sur les Bourses »

M – *The Guardian*, 25/01/2014, « Gmail outage hits millions across the world, including UK, US & India »

M – site *IT Pro Portal*, 26/03/2014, « The cybercrime economy could be bigger than Apple, Google and Facebook combined »

D – Kroll Ontrack, 28/02/2014, « Global data theft worse than expected »

M – site *SFgate*, 24/01/2013, « The underground economy of cybercrime »

M – *CNBC*, 13/08/2013, « The threat from cybercrime? You ain't seen nothing yet »

M – *Le Figaro*, 2/10/2013, « La sécurité informatique prend un nouveau tournant »

M – *The Guardian*, 31/10/2013, « Online fraud costs global economy many times more than $100 bn »

M – site *Maximum PC-Symantec*, 10/04/2014, « Cybercriminals shift behavior to mega breaches in hope of better payment »

M – *La Tribune,* 16/06/2014, « L'e-commerce ne connaît pas la crise »

M – *Thanh Nien News Vietnam*, 26/05/2014, « Vietnam among world's biggest cybercrime victims »

D – Cyber Security Conference, 26/02/2014, San Francisco – James Comey, director FBI

M – *National Jeweller*, 7/06/2013, « Use of violence in retail crimes on the rise »

M – *Business Insider*, 20/03/2014, « California leads the nation in cybercrime »

M – *Dark Reading*, 12/09/2013, « Medical ID theft spreads »

M – *Dark Reading*, 4/11/2013, « Study: data of more than 16 million Americans compromised by breaches last year »

M – *New York Times International*, 4/03/2014 – « US powergrid is called vulnerable to cyberattacks »

M – *IT World*, 7/01/2013, « EU organized crime makes € 1,5 billion a year »

D – *European Commission*, 20/06/2014, « Communication from the Commission to the European parliament and the Council – The final implementation report of the EU internal security strategy »

M – *La Tribune*, 24/07/2014, « Vols de données à la BCE : jusqu'à 20 000 personnes potentiellement concernées »

M – *The Independent*, 24/07/2014, « Hackers demand ransom after stealing personal data from European central bank »

D – UK – Home Office, 02/2014, « Crime against businesses – headline findings from the 2013 commercial victimization survey »

M – *The Independent*, 31/03/2013, « Cybercrime, the focus of a new government security initiative »

M – *Daily Mail*, 25/04/2013, « Britain under attack: cybercrime… »

M – *BBC News*, 30/07/2013, « UK "losing fight" against Internet crime, warns MP's »

M – *The Guardian*, 23/08/2013, « Cybercrime hits more than 9 million UK web users »

M – *Le Figaro*, 29/04/2011, « Explosion des arnaques à la carte bancaire en France »

M – *Le Monde*, 8/05/2014, « Orange de nouveau victime d'une cyberattaque massive »

M – *Le Parisien*, 10/01/2012, « Les fraudes à la carte bancaire en 2011 »

M – *Le Parisien*, 10/01/2013, « Carte bancaire : les débits frauduleux explosent sur Internet »

M – *Le Figaro*, 3/07/2013, « La fraude à la carte bancaire continue de progresser légèrement »

M – *Le Figaro*, 27/09/2013, « Les cyberattaques ont doublé depuis 2010 »

M – *Le Parisien*, 2/02/2014, « Orange : les données personnelles de 800 000 clients piratées »

M – *Le Parisien*, 30 avril 2014, « Cyberattaques : la France, cible privilégiée de hackers chevronnés »

M – *Agence France Presse*, 15/07/2014, « Le montant des fraudes à la carte bancaire en hausse »

M – *RTE News*, 3/04/2014, « Cybercrime cost Irish economy € 630 million a year »

M – *Deutsche Welle*, 28/01/2013, « Online gambling: playing into the mafia's hands ? »

M – *Intelligence Brief*, 16/09/2013, « Attaque sur Vodafone Allemagne »

M – *Le Parisien*, 21/01/2014, « Allemagne : 16 millions de boîtes mail piratées »

M – *The Local Deutschland*, 24/01/2014, « How to hack 16 million email accounts »

M – *The Local Deutschland*, 3/06/2014, « Police struggle as cybercrime hits record »

M – *ZD Net*, 29/01/2013, « China looses US$ 46 billion to cybercrime in 2012 »

M – *BBC News*, 4/03/2014, « China cybergangs use vast underground networks »

M – *PC Advisor*, 8/07/2013, « Cybercrime becomes more prevalent in Hong Kong »

M – *Reuters*, 21/04/2014, « Panique en Corée du sud après un piratage massif de données bancaires »

M – *Le Monde*, 23/01/2014, « Vol massif de données bancaires en Corée du Sud »

M – *ZD Net*, 23/10/2013, « India ransomware capital of APAC… »

M – « Vietnam among world's biggest cybercrime victims » (*op. cit*.)

M – *Reuters*, 8/07/2014, « Nigerian scammers have made Malaysia the new epicenter of online crime »

M – *The National* (Abu Dhabi), 28/01/2014, « Cybercrime in Dubai nearly double in 2013 »

M – *Insight*, 10/04/2014, « Mexico cybercriminals "kidnapping" business computer systems »

M – *Info Sur Hoy*, 11/04/2014, « Mexico : computer hacking becoming form of extortion »

M – *Insight*, 2/07/2014, « Mass online theft in Brazil sheds light on scale of cybercrime »

M – *New York Times International*, 3/07/2014, « Brazilians are target of cybercrime operations »

M – *Insight*, 19/06/2014, « Hacker group arrest in Colombia points to evolution in cybercrime »

M – *Insight*, 11/07/2014, « Cybercrime in Colombia: an underestimated threat ? »

D – Délégation aux Affaires stratégiques, 09/2013, « Observatoire trimestriel du monde cybernétique »

M – *Agence France Presse*, 18/06/2014, « Roumanie : un réseau cybercriminel démantelé »

M – *BBC News*, 2/06/2014, « Russian Evgeniy Bogatchev sought over cybercrime botnet »

M – *Le Figaro*, 3/06/2014, « Un très puissant réseau de cybercriminels démantelé »

L – Julia Angwin, *Dragnet nation – a quest for privacy, security and freedom in a world of relentless surveillance*, Times Books, 2014

M – *The Daily Beast*, 3/08/2013, « Ransomware scams prey on your sense of guilt to open your wallet »

M – *New York Review Of Books*, 9/01/2014, « How your data are being deeply mined »

D – Symantec, 1/10/2013, « 2013 Norton Report: cost per cybercrime victim up 50 % »

M – *Le Figaro*, 5/05/2014, « La voiture, nouvelle cible des pirates informatiques »

M – *Network World*, 9/10/2013, « Most costly cybercrime attacks: denial-of-service malicious insider and web based »

M – *CBS*, 22/08/2013, « Crooks use cyberattacks on banks to steal millions »

M – *Reuters*, 27/05/2013, « US indicts hackers in biggest cyberfraud case in history »

M – *International Herald Tribune*, 21/09/2013, « 8 arrested in Barclays branch cybertheft »

M – *Los Angeles Times*, 31/05/2013, « Some companies looking at retaliating against cyber attackers »

M – *Associated Press*, 21/05/2014, « Prévention du piratage : l'énorme défi du FBI »

M – *Le Monde*, 25/05/2014, « Les entreprises et leurs fichiers clients, cibles de choix des pirates informatiques »

M – *L'Express,* 8/05/2014, « Cyberattaques : un nouveau marché prometteur pour les assurances »

M – *New York Times International*, 3/03/2014, « Data security is no longer on the back burner »

M – *Le Figaro,* 10/03/2014, « Les entreprises face au défi de la sécurité informatique »

M – *Le Figaro*, 22/01/2014, « Les banques pas assez réactives face au piratage des comptes bancaires »

M – *Agence France Presse*, 10/04/2014, « La finance et les médias US, cible des hackers »

M – *Daily Telegraph*, 22/05/2014, « The biggest ever cyberattacks and security breaches »

M – site *Krebs On security*, 10/04/2014, « Experian lapse allowed ID theft service access to 200 million customer records »

M – *Information week*, 11/03/2014, « Experian ID theft exposed 200 m. consumer records »

M – *Daily Telegraph*, 21/05/2014, « More than 15 million Britons at risk of identity theft after eBay hacked »

M – *Associated Press*, 21/05/2014, « eBay victime de pirates informatiques »

M – *Daily Mail*, 23/05/2014, « Hacked eBay can only be fined up to £ 500 000 for breach of its data ».

M – *Le Monde*, 23/05/2014, « eBay, nouvelle victime des pirates informatiques »

M – *Agence France Presse*, 18/06/2014, « Les entreprises, de plus en plus rançonnées par les hackers »

M – *Le Point*, 16/06/2014, « Domino's Pizza refuse de payer une rançon »

M – *Le Figaro*, 16/06/2014, « En plein mondial, Domino's Pizza se fait hacker les données de ses clients »

# PARTIE 4 – LA CYBERCRIMINALITÉ EN ACTION

L – Ulrich Beck, *La société du risque*, Champs Flammarion, 2001

L – Charles Seife, *Virtual unreality*, Viking, 2014

M – *Foreign Policy*, 19/07/2013, « Mobs rule – why organized crime is a growing force in world politics »

M – « Dozens held in Philippines over global "sextortion" ring » (*op. cit*.)

M – *Time mag.* 11/11/2013, « The Deep web »

M – *Le Monde*, 28/05/2014, « Monnaies électroniques – la mode du dark »

M – *Atlantico*, 17/03/2014, « Comment créer son propre site sur le deep web »

M – *Network World*, 2/04/2014, « Dark web : an evermore comfortable haven for cybercriminals »

M – *New York Times International*, 17/02/2014, « Blogging, with a shotgun at his side, about the web's criminal underbelly »

M – *Reuters*, 26/08/2013, « Ex-soviet hackers play outsized role in cybercrime world »

M – *NBC News*, 5/02/2014, « Skilled, cheap russian hackers power American cybercrime »

M – *Security Defense Business Review*, 25/03/2014, « TOR, réseau favori des cyber-délinquants »

M – site *V3.CO. UK*, 9/04/2014, « Criminals launching TOR alternatives to avoid detection »

M – *Le Monde*, 3/07/2014, « TOR, logiciel-clé de protection de la vie privée, dans le viseur de la NSA »

M – *L'Express*, 28/07/2014, « Qui sera l'œil de Moscou sur le réseau anonyme TOR ? »

M – *BBC News*, 23/07/2014, « TOR project makes effort to debug dark web »

M – *WMBF*, 6/02/2013, « Robberies decrease as cybercrime increases, FBI says »

M – *CNN – Money – Cybercrime economy*, 9/07/2013, « Cyberattacks are the bank robberies of the future »

M – *International Herald Tribune*, 11/05/2013, « International ATM heist nets $ 45 million for gang of laptop hackers »

M – *Dark Reading*, 30 avril 2014, « Interpol assisted information exchange among investigators worldwide in USD 45 million theft »

M – *ZD Net*, 26/03/2014, « Hackonomics: cyber black market more profitable than illegal drug trade »

M – *Agence France Presse*, 11/07/2014, « Coupable d'une attaque à 14 millions »

M – *Le Figaro*, 13/04/2014, « Heartbleed: la faille qui frappe le cœur de la sécurité sur Internet »

M – *Le Monde*, 6/06/2014, « Après Heartbleed, une nouvelle faille de sécurité dans OpenSSL »

M – *Marketplace Morning Report,* 7/10/2013, « Hacking and the value of a zero day »

M – *Insight*, 26/02/2014, « Kidnap cybercrime techniques spread to Bolivia »

M – *Le Monde*, 16/04/2014, « Les cybermenaces n'ont pas disparu »

M – *BBC News*, 16/10/2013, « Police warning after drug traffickers cyber-attack »

M – *International Herald Tribune*, 17/07/2013, « Cyberattacks rise steeply at American universities »

M – *Associated Press*, 15/01/2014, « Prosecutor: Florida tops US in identity theft, tax fraud »

M – *Associated Press*, 8/01/2014, « IRS: identity theft prosecutions double in 2013 »

M – *Washington Post*, 5/02/2014, « Cyberattacks are on the rise and health care data is the biggest target »

M – *PR web*, 10/03/2014, « Filing fraudulent tax returns nets nearly $ 4 billion payday for cybercriminals »

M – *CNET*, 14/04/2014, « Personal data theft jumps from 11 % to 18 % in six months »

M – *GigaOM*, 22/08/2013, « Your identity is probably worth $ 5 on the black market »

M – *Computer Weekly*, 4/03/2014, « Identity theft linked to 60 % of UK fraud in 2013 »

M – *Sydney Morning Herald*, 27/01/2013, « Identities for sale: fake documentation on the rise »

M – *International Business Times*, 1/04/2014, « DDoS attacks rise by 240 % in 2014, says security watchdog »

M – *Professional Security Magazine Online/UK*, 4/04/2014, « Fraud figures rise »

M – site *Krebs On Security*, 27/03/2014, « Who built the ID theft service SSNDOB.ru ? »

M – *USA Today*, 28/01/2014, « If the credit charge was $ 9.84, take a closer look »

M – *Computer World*, 19/09/2013, « Hacking courses offer cybercrooks tips on how to hone skills »

M – *Dark Reading*, 4/11/2013, « Dark side services continue to grow and prosper »

M – site *webroot Threat Blog*, 23/09/2013, « Cybercriminals sell access to tens of thousand of malware-infected Russian hosts ».

M – *webroot Threat Blog*, 7/02/2014, « Market leading standardized cybercrime friendly e-shop service brings 2 500+ boutique e-shop online »

M – site *Phys.org*, 25/03/2014, « Cybercrime part of a sophisticated online economy, study says »

M – *Information Week*, 26/03/2014, « Cybercrime black markets grow up »

M – *webroot Threat Blog*, 7/11/2013, « Source code for proprietary spam bot offered for sale »

M – *Tech Week Europe*, 26/03/2014, « Cybercrime industry runs its own marketing, recruitment and customer service »

M – *Wall Street Journal*, 30/09/2013, « Phony web traffic tricks digital ads »

M – *New York Times International*, 12/04/2014, « Bot armies are on the march across the Internet, and getting smarter »

M – *Le Monde*, 12/08/2014, « Près d'un compte Twitter sur 10 est alimenté par un robot »

M – *USA Today*, 16/01/2014, « Google steps up fight against "bad" ad barrage »

M – *The Guardian*, 28/08/2013, « Facebook spammers make $ 200 million just posting links »

M – *New York Times International*, 2/09/2013, « Online attacks leads to peek into spam den »

M – *Le Monde*, 25/05/2014, « Vaste coup de filet contre les utilisateurs d'un logiciel grand public de piratage »

M – *Nouvel Observateur*, 20/05/2014, « Blackshades : le piratage passe à l'ère industrielle »

M – *CNN*, 19/05/2014, « More than 90 people nabbed in global hacker crackdown »

M – *Dark Reading*, 30/05/2014, « Blackshades boss pleads not guilty »

M – *Forbes*, 6/08/2012, « Black market drug site Silk Road booming: $ 22 million in annual sales »

M – *Esquire*, 3/10/2013, « Meet the Internet $ 80 million kingpin »

M – *Chicago Sun-Times*, 9/05/2014, « World's most prolific online drug dealer »

M – *Le Monde*, 7/11/2013, « Le site illégal Silk Road recréé un mois après sa fermeture par le FBI »

M – *New York Times International*, 18/11/2013, « Dark web of crime, anonymous and growing »

M – *New York Times International*, 20/01/2014, « On the trail of an online drug mastermind »

M – *Dark Reading*, 30/10/2013, « Cybermonday attacks cost enterprises up to 3,4 million per hour »

M – *Financial Times*, 20/12/2013, « Credit card data stolen from 40 m. shoppers at big US retailer target »

M – *Los Angeles Times*, 21/12/2013, « Target reels under huge data breach »

M – *New York Times International*, 15/03/2014, « Target chain disregarded warnings of a data breach »

M – *New York Times International*, 12/02/2014, « Dogged by data theft »

M – *webroot Threat Blog*, 21/02/2014, « Can security survive in an increasingly insecure world »

D – *Verizon Risk Report*, 2013

M – *Business Insider*, 7/04/2014, « Russian cybercrime syndicate linked to Neiman Marcus theft »

# PARTIE 5 – A L'HORIZON, TROIS QUESTIONS MAJEURES

M – Communiqué du Parlement européen, 13/02/2014, « Espionnage de la NSA – des propositions pour protéger la vie privée des citoyens européens »

M – *New York Review Of Books*, 15/08/2013, « They know much more than you think »

D – Privacy and civil liberties oversight board, 23/01/2014, « Report on the telephone records program… »

D – Rapport, décembre 2013, « President's review group on intelligence and communications technology »

M – *Wall Street Journal*, 3/08/2013, « FBI taps hacker tactics to spy on suspects »

M – *International Herald Tribune*, 24/08/2013, « Pentagon is scouted for frontline expertise on cybersecurity »

M – *The Guardian*, 7/03/2014, « The NSA is screwing up the fight against cybercrime »

M – *New York Times International*, 15/01/2014, « NSA able to penetrate computers not on web »

M – *International Herald Tribune*, 7/09/2013, « NSA foils encryption protection around globe »

M – *Nouvel Observateur*, 24/07/2014, « États-Unis : la liste noire dressée sur de simples soupçons »

M – *The Guardian*, 18/11/2013, « Private firms selling mass surveillance systems around world, document show »

M – *International Herald Tribune*, 12/08/2013, « Emails firms close rather than share data »

M – *International Herald Tribune*, 31/08/2013, « Budget leak reveals US spending on intelligence »

M – *GBC*, 29/08/2013, « Leaked spy's budget's three most revealing parts »

M – *La Tribune*, 21/05/2014, « NSA : combien coûte le stockage des appels téléphoniques ? »

M – *New York Review Of Books*, 19/06/2014, « Can the NSA be controlled ? »

M – *New York Times International*, 29/06/2014, « NSA chief says that damage from Snowden leaks is manageable »

M – *Agence France Presse*, 1/07/2014, « La NSA espionnait 193 pays »

M – *L'Express*, 7/07/2014, « 90 % des citoyens espionnés par la NSA sont des gens ordinaires ».

M – *New York Times International*, 7/06/2014, « Eyes and ears everywhere »

M – *Le Figaro*, 6/06/2014, « De Prism à TOR, les dix noms du scandale de la NSA »

M – *The Guardian*, 10/07/2014, « One of the NSA original whistleblowers says the goal is "total population control" »

M – *New York Times International*, 1/08/2014, « Westerners who turn to terror prove hard to track »

M – *New York Review Of Books*, 10/07/2014, « Partial disclosure »

M – *Washington Times*, 30/07/2014, « The next 9/11 could be a cyber-attack »

M – *Le Figaro*, 21/05/2014, « Comment le FBI a traqué les cybersoldats chinois »

M – *New York Times International*, 15/07/2014, « Chinese hackers extending reach to smaller US agencies, officials say »

M – *Financial Times*, 6/05/2014, « Foreign spy agencies recruiting big business IT staff, warns MI 5 »

M – (« Cybersecurity and cyberwar – what everyone needs to know », *op. cit*.)

M – *New York Times International*, 31/05/2014, « Iran linked to intricate cyberspying campaign »

M – *International Herald Tribune*, 27/05/2013, « Wave of computer attacks in US traced back to Iran »

M – *Communication et Influence*, juin 2014, « Entretien avec Yves Lacoste »

M – *Yale journal of International Affairs*, Hiver 2013, « Cyberwar in the underworld: anonymous versus Los Zetas in Mexico »

M – *International Herald Tribune*, 29/06/2013, « US retools approach to cyberwar »

M – *Agence France Presse*, 23/07/2014, « Les USA pas à l'abri d'un cyber-11 septembre »

M – *International Herald Tribune Magazine*, Turning Points 2014, 27/11/2013, « Cyber subterfuge »

M – *RUSI Journal*, 8/09/2013, « The sophistication criterion for attribution – identifying the perpetrators of cyber-attacks »

M – *RUSI Journal*, 8/09/2013, « Warrior geeks – how 21st century technology is changing the way we fight and think about war »

M – *International Herald Tribune*, 2/09/2013, « US files point to big offensive in cyberspace »

D – *National Security Program* – Homeland Security Project, July 2014, « Reflections on the tenth anniversary of the 9/11 commission report »

M – *Agence France Presse*, 6/01/2014, « Les cyberattaques, première menace selon les responsables de la défense US »

M – *Le Monde*, 13/08/2014, « L'Ukraine et la Russie au bord de la cyberguerre »

M – *Le Monde*, 7/04/2014, « Des hackers ont visé des futurs fonctionnaires américains habilités au "secret-défense" »

D – *Committee on offensive information warfare*, National research council, Washington DC, National Academies Press, 2009, « Technology policy, law and ethics regarding US acquisition and use of cyberattack capabilities »

M – *Studies in conflict and terrorism*, mars 2014, « The cyberterrorism threat: findings from a survey of researchers »

M – *Armées d'aujourd'hui*, 7/08/2013, « L'Europe prend en main sa cybersécurité »

M – *Sécurité Défense Business Review*, 24/09/2013, « Interview du contre-amiral Arnaud Coustillière, officier général cyberdéfense, état-major des armées »

M – *Le Point*, 29/01/2014, « Cyberguerre : nos armes informatiques sont opérationnelles »

M – *Le Figaro*, 6/08/2014, « La lutte contre al cybercriminalité est un marché d'avenir »

M – *New Scientist*, 12/10/2011, « Cops on the trail of crimes that haven't happened »

M – *New York Times-web*, 15/08/2011, « Sending the police before there's a crime »

M – *National Public Radio*, 26/11/2011, « At LAPD, predicting crimes before they happen »

D – Vineland NJ Police department, 5/07/2011, « To predict and serve : predictive intelligence analysis »

M – *Atlantic Cities Online*, 14/03/2012, « How to catch a criminal with data »

M – *International Herald Tribune*, 24/11/2012, « Giant steps in teaching computers to think like us »

M – *Euronews*, 25/02/2013, « Forecasting crime »

M – *Le Monde* – Blog, 23/08/2013, « Grâce à Wikipedia, il est possible de prédire le succès – ou pas – d'un film »

M – site *International.to*, 4/03/2013, « Future planet – future of surveillance »

L – Anasse Bari, Mohamed Chaouchi, Tommy Jung, *Predictive analytics for dummies*, Wiley, NJ, 2013

M – *Le Figaro*, 21/01/2014, « La drôle de machine de “person of interest” »

M – *Journal du Dimanche*, 3/03/2014, « La machine à déceler le crime »

M – *Wired*, 11/2013, « Future of War »

L – Eric Siegel, *Predictive analytics – the power to predict who will click, buy, lie or die*, Wiley ed. NJ, 2014

M – *Le Monde*, 12/04/2014, « Big brother, ce vendeur »

M – *Seattle Times*, 28/02/2013, « Seattle police turn to computer software to predict, fight, crime »

M – *Salon*, 13/03/2013, « Predictive policing technology spreads on West coast »

M – site *Prison Planet*, 14/03/2013, « Cops patrolling Facebook for predictive policing »

M – *Geekwire*, 18/05/2013, « Anticipating where crime happens: Seattle rolls out “predictive policing” »

M – *Insight*, 3/07/2013, « Chile engineers calculate crime hotspots »

M – *Business Insider*, 10/07/2013, « How students used Big Data to analyze crime in San Francisco »

M – *Le Point*, 20/04/2014, « Et si Twitter aidait à prévenir la criminalité ? »

M – *Agence France Presse*, 19/04/2014, « Researchers use Twitter to predict crime »

M – *Business Insider*, 19/03/2014, « These maps show how Twitter can be used to predict crime down to the city block »

M – site *Brazil Tech*, 21/04/2014, « Sao Paulo invests $ 4,3 m. in Microsoft crime fight system »

M – *The Economist*, 17/04/2014, « Parole and technology: prison breakthrough »

M – *New York Times,* 11/08/2014, « Sentencing by the numbers »

D – Princeton University, 02/2011, Danziger, Levav, Avnaïm-Pesso – « Extraneous factors in judicial decisions »

M – *New York Review Of Books*, 9/01/2014, « Donald Rumsfeld revealed »

M – *Le Monde-Blogs*, 14/03/2014, « La conception algorithmique automatise-t-elle nos vies ? »

M – *Le Monde*, 31/05/2014 « Un "Big Data" socialement utile »

M – *Le Monde*, 29/01/2014, « Big data, trois défis pour les maths »

M – *American Public Radio* – Freakonomics Radio, 31/03/2011, « Why can't we predict earthquakes ? »

M – BBC News, 29/07/2014, « OK Cupid: who believes compatibility ratings on dating websites »

M – *International Herald Tribune*, 7/02/2013, « Trails of scandals: altering models to boost the results »

M – *New York Times International*, 21/07/2014, « Who routinely beats the market ? No none »

M – *International Herald Tribune*, 27/09/2013, « In search of "quant" genius, hedge funds turn to contests »

M – *Daily Bwin* (UCLA, quotidien), 26/04/2013, « Professor helps develop predictive policing by using trends to predict, prevent, crime »

M – *The Guardian*, 25/06/2014, « The LAPD is predicting where crime will occur based on computer analysis »

# PARTIE 6 – PRESCRIRE

M – *Courrier Militaro-Industriel* (Moscou), 27/02/2013, « The value of science in prediction » – Général Valéry Gerasimov, chef d'état-major général, Russie

M – *Bloomberg*, 10/06/2013, « Pentagon five-years cybersecurity plan seeks $ 23 billion »

M – *Washington Post*, 27/01/2013, « Pentagon to boost cybersecurity forces »

M – *New York Times International*, 9/06/2014, « Cyberinsurance, an industry still finding its way »

M – *New York Times International*, Bits Special Report, 13/06/2014 – « The dangers of leaving the office »

M – *New York Times International*, 22/07/2014, « The job that asks: can you hack it? »

M – *Paris Match*, 21/01/2014, « Fou-rire chez les hackers – le classement mondial des mots de passe »

M – *Sécurité Défense Business Review*, 11/03/2014, « 3 questions à Jean-Christophe Vitu… »

M – *Sécurité Défense Business Review*, 22/10/2013, « Les assises de la sécurité et des systèmes d'information »

M – *Sécurité Défense Business Review*, 3/12/2013, « Interview de Laurent Hesbault, security strategist at Symantec »

M – « Cyberattaques : la France, cible privilégiée de hackers chevronnés » (*op. cit*.)

D – Spécial Eurobarometer-390, July 2012, « Cyber security report »

M – *Financial Times*, 21/05/2014, « A new breed of cyber spy tackling hackers on their own turf »

M – Michael Brenner Blog, 25/08/2013, « The only alternative – and other possibilities »

M – *International Herald Tribune*, 29/07/2013, « When web magnifies bad data »

M – *NBC News*, 12/04/2014, « Boston legacy: can crowdsourcing really fight crime ? »

M – *Associated Press*, 2 mai 2014, « Police are gathering evidence through the cloud »

M – *New York review Of Books*, 15/08/2013, « The man who got it right »

M – *Les Echos*, 1/08/2013, « Les champs de bataille de la guérilla numérique »

# CONCLUSION : L'AVENIR RADIEUX DU CYBERCRIME

M – *La Tribune*, 21/01/2014, « Cybercriminalité : 3 000 milliards de dollars de pertes pour l'économie d'ici 2020 »

M – *Dark Reading*, 22/07/2014, « 7 Black Hat sessions sure to cause a stir »

M – *Wired*, 24/07/2014, « How hackers hid a money-mining botnet in the clouds of Amazon and others »

M – « Dozens held in Philippines over global "sextortion" ring » (*op. cit*.)

M – *Financial Times*, 24/05/2014, « Hacked off »

M – *Libération*, 12/05/2014, « Objets connectés : tous hackés ? »

M – *Le Parisien*, 18/01/2014, « Sécurité Informatique : des pirates attaquent des télés et un frigo »

M – *New York Times International*, 2/06/2014, « Dark side to the Internet of things: hacked homes and invasive ads »

M – *Bloomberg*, 22/04/2014, « What happens when the "Internet of things" comes to ATM skimmers »

M – *International Herald Tribune*, 13/08/2013, « With computers controlling our cars, hackers intrusion could turn deadly »

M – *International Herald Tribune*, 14/09/2013, « Drivers begin to take a back seat »

M – *Le Figaro*, 8/09/2013, « Alan Mulally : la voiture devient un terminal Internet, comme un smartphone »

M – *New York Times International*, 4/07/2014, « Look Ma, no hands: trucking's future »

M – *International Herald Tribune*, 22/08/2013, « Facial scanning makes advances »

M – *Dark reading*, 28/01/2014, « DDoS just won't die »

M – *Dark reading*, 2/06/2014, « Global effort disrupts GOZeuS botnet, Cryptolocker, one indicted »

M – *Krebs On Security*, 10/07/2014, « Crooks seek revival of GameoverZeuS botnet »

M – *New York Times International*, 2/07/2014 (pages spéciales Russie), « Aiming to secure the cyber-future »

M – *Agence France Presse*, 6/08/2014, « Des pirates informatiques russes auraient volé plus d'un milliard de mots de passe »

M – *New York Times International*, 6/08/2014, « Hackers steal huge trove of virtual data »

M – *BBC News*, 11/08/2014, « Do quantum computers threaten global encryption systems? »

Retrouvez tous les ouvrages de CNRS Éditions
sur notre site www.cnrseditions.fr

This file was downloaded from Z-Library project

*Your gateway to knowledge and culture. Accessible for everyone.*

z-library.sk z-lib.gs z-lib.fm go-to-library.sk

Official Telegram channel

Z-Access

https://wikipedia.org/wiki/Z-Library